NETGEAR ProSafe SSL VPN Concentrator 25 SSL312 Reference Manual

NETGEAR®

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10208-01
August 2006

Technical Support

Please register to obtain technical support. Please retain your proof of purchase and warranty information.

To register your product, get product support or obtain product information and product documentation, go to *http://www.NETGEAR.com*. If you do not have access to the World Wide Web, you may register your product by filling out the registration card and mailing it to NETGEAR customer service.

You will find technical support information at: *http://www.NETGEAR.com/* through the customer service area. If you want to contact technical support by telephone, see the support information card for the correct telephone number for your country.

Trademarks

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

FCC Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Requirements for Operation in the United States

Radio Frequency Interference Warnings & Instructions This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help.

RF Exposure Warning for North America, and Australia

Warning! To ensure compliance with FCC RF exposure requirements, the antenna used for this device must be installed to provide a separation distance of at least 20 cm (8 in) from all persons and must not be co-located or operating in conjunction with any other antenna or radio transmitter. Installers and end-users must follow the installation instructions provided in this user guide.

EU Regulatory Compliance Statement

ProSafe SSL VPN Concentrator 25 is compliant with the following EU Council Directives: 89/336/EEC and LVD 73/23/EEC. Compliance is verified by testing to the following standards: EN55022 Class B, EN55024 and EN60950.

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSafe SSL VPN Concentrator 25 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß dasProSafe SSL VPN Concentrator 25 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Product and Publication Details

Model Number:	SSL312
Publication Date:	August 2006
Product Family:	Concentrator
Product Name:	ProSafe SSL VPN Concentrator 25
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10208-01
Publication Version Number:	1.0

Contents

About This Manual

The *NETGEAR® Prosafe™ SSL VPN Concentrator 25 SSL312 Reference Manual* describes how to install, configure and troubleshoot the ProSafe SSL VPN Concentrator 25. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions.** This manual uses the following typographical conventions:

Italics	Emphasis, books, CDs, URL names
Bold	User input
`Fixed`	Screen text, file and server names, extensions, commands, IP addresses

- **Formats.** This manual uses the following formats to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

Tip: This format is used to highlight a procedure that will save time or resources.

Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.

	**Danger:** This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope.** This manual is written for the SSL VPN Concentrator according to these specifications:

Product Version	ProSafe SSL VPN Concentrator 25
Manual Publication Date	August 2006

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, "Related Documents".

	**Note:** Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/SSL312.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons,  and  , for browsing forwards or backwards through the manual one page at a time
- A  button that displays the table of contents and an  button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A  button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Page in the HTML View**.

Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a Chapter**.

  Use the *PDF of This Chapter* link at the top left of any page.

  – Click the *PDF of This Chapter* link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

  – Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

  – Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

- **Printing the Full Manual**.

  Use the *Complete PDF Manual* link at the top left of any page.

  – Click the Complete PDF Manual link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.

  – Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 1
Introduction

This chapter describes some of the key features of the NETGEAR® ProSafe™ SSL VPN Concentrator 25 SSL312. It also includes the minimum prerequisites for installation and ("Web Browser Requirements" on page 1-2.), package contents ("What's in the Box" on page 1-3), and a description of the front and back panels of the SSL312 ("Hardware Description" on page 1-3). The default SSL VPN Concentrator address is **http://192.168.1.1**.

About the ProSafe SSL VPN Concentrator 25

The ProSafe SSL VPN Concentrator 25 is an innovative hardware-based SSL VPN solution designed specifically to provide remote access for mobile users to their corporate network, without requiring a VPN client on their systems. The Secure Sockets Layer (SSL) protocol operates between TCP/IP and application protocols such as HTTP and FTP allowing a secure server to authenticate itself to an SSL-enabled client, such as a web browser. Once the authentication and negotiation of encryption information is completed, the server and client can establish an encrypted connection. With support for 25 concurrent sessions, users can easily access the remote network and enjoy a customizable, secure, user portal experience from virtually any available platform.

The ProSafe SSL VPN Concentrator 25 is an innovative hardware-based SSL VPN solution designed to provide remote access to corporate resources. Supporting Secure Sockets Layer (SSL), a protocol that operates at the application layer, the SSL VPN Concentrator allows users to access corporate resources remotely without requiring a pre-installed client on their laptops.

Key Features

The ProSafe SSL VPN Concentrator 25 is easy to use and to administer, through a customizable and intuitive interface. Other key features:

- Uses Secure Sockets Layer (SSL) protocol to transfer data. SSL is a protocol that is extensively used in the world of electronic commerce and has gone through years of public scrutiny.

- Connects to the SSL VPN Concentrator through a number of popular browsers, such as Microsoft Internet Explorer or Apple Safari.
- Supports 25 concurrent sessions.
- Provides granular access to corporate resources based upon user type or group membership.
- Supports multiple user authentications, including local database, Microsoft Active Directory, LDAP, NT Domain and RADIUS.
- Provides client-less access with customizable user portals and support for a wide variety of user repositories. Access includes support for:
  - Full network access
  - HTTP and HTTPS proxy and reverse proxy
  - Remote Desktop and Application Access including File Sharing
- Browser based, platform-independent, remote access using Microsoft Internet Explorer and Apple Safari.

Web Browser Requirements

The following web browsers are supported for the SSL VPN Concentrator web management interface and the SSL VPN portal. Note that Java is only required for the SSL VPN portal, not the web management interface.

- **Microsoft Windows:**
  - **Browsers:** Internet Explorer 6.5.1.or higher
    Mozilla 1.x (administrator only)
  - **Java:** Sun JRE 1.1 or higher
    Microsoft JVM 5 or higher
- **Apple MacOS X:**
  - **Browser:** Safari 1.2 or higher
  - **Java:** Sun JRE 1.1 or higher
- **Unix, Linux, or BSD:**
  - **Browser:** Mozilla 1.x (administrator only)
    Safari 1.2 or higher
  - **Java:** Sun JRE 1.1 or higher

To configure the NETGEAR ProSafe SSL VPN Concentrator 25, an administrator must use an Internet Explorer 6.5.1 or higher, Apple Safari 1.2 or higher, or Mozilla l.x web browser with **JavaScript**, **cookies**, and **SSL-enabled**.

What's in the Box

The product package should contain the following items:

- ProSafe SSL VPN Concentrator 25 SSL312
- A power cord specific to your region.
- Straight through Category 5 Ethernet cable.
- A serial cable.
- *Resource CD*
- *ProSafe™ SSL VPN Concentrator 25 SSL312 Installation Guide*
- Warranty and Support Registration Card

Hardware Description

This section describes the front and rear hardware functions of the SSL312.

Front Panel

The SSL VPN Concentrator front panel hardware is shown in Figure 1-1 below:

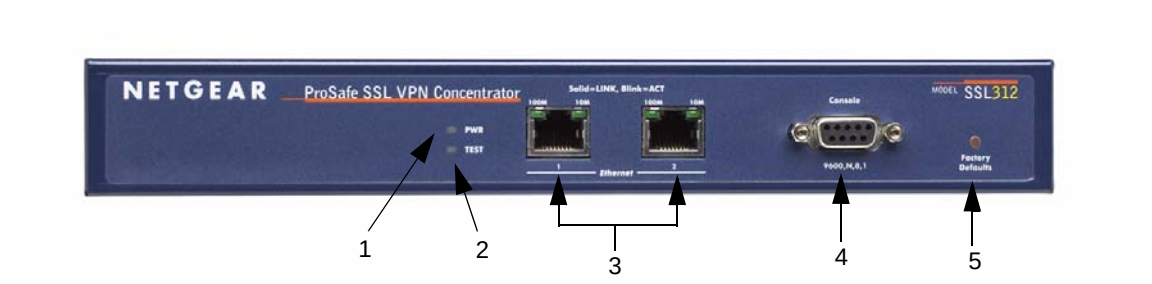

Figure 1-1

The SSL VPN Concentrator front panel hardware functions are described below:

1. LED Power Indicator:
   - Off – No power
   - On – Power is on.
2. LED Self test Indicator.
   - Self test – on while initializing. (~2 minutes)
   - Loading Software – blinking while uploading software
   - System fault – on (prolonged)

   This LED may blink for a minute before going off.
3. Two 10/100M Ethernet ports:
   - A solid green LED indicates a connectivity link has been established on either the 10M or 100M interface.
   - A blinking green LED indicates activity on either the 10M or 100M interface.
4. Serial Console Port

   Male DB-9 serial port for serial DTE connections.
5. Restore to Factory Defaults Button

Back Panel

The SSL VPN Concentrator back panel hardware is shown in Figure 1-2 below and consists of the power On/Off switch and the 110-240V power cord connection.

Figure 1-2

	Note: Never substitute a power cord. Only use the power cord provided with the SSL VPN Concentrator.

Chapter 2
Basic Installation and Configuration

The initial administrative setup of the ProSafe SSL VPN Concentrator 25 must be performed using an Internet Explorer Browser 6.5.1 or higher, Apple Safari 1.2 or higher, or Mozilla 1.x. End Users can use IE 6.5.1 or higher or Apple Safari 1.2 or higher. The browsers should also support JavaScript, Java, cookies, SSL and ActiveX to take advantage of the full suite of applications.

Note: End Users can open and use a Mozilla 1.x browser after an initial connection has been made using IE or Safari. If the IE or Safari browser is closed, the connection will be lost.

Installing the SSL VPN Concentrator

Before installing the ProSafe SSL VPN Concentrator 25, make sure that your Ethernet network is up and working. The ProSafe SSL VPN Concentrator 25 is a browser-based portal that connects to your Ethernet network.

To set up the SSL VPN Concentrator:

1. Prepare a PC with an Ethernet adapter. If this PC is already part of your network, record its TCP/IP configuration settings.
2. Configure your PC with a static IP address of 192.168.1.10 and 255.255.255.0 as the subnet mask.
3. Connect an Ethernet cable from your computer to Ethernet Port 1 on the front of the SSL VPN Concentrator.
4. Connect the power cord to the SSL312, turn on the concentrator and verify the following:
   - The PWR power light goes on.
   - The system has initialized and the TEST light has gone off.
   - One of the LAN lights is lit: either the 10 Mbps or the 100 Mbps LED should light showing that a connectivity link as been established

Configuring the ProSafe SSL VPN Concentrator 25

After the ProSafe SSL VPN Concentrator 25 software has been installed and the Static IP address configured, you may log into the SSL VPN Concentrator web management interface from an IE 6.5.1 or higher, Safari 1.2 or Mozilla 1.x. The machine used for management is referred to as the "Management Station".

	Note: You must have administrative access to your network's concentrator device to configure the Management Interface settings

To log into the management interface:

1. Connect to the SSL312 by opening your browser and entering **https://192.168.1.1** (for the Ethernet Port 1 IP) in the address field. .

Figure 2-1

If you are connected to Ethernet Port 2 IP, the default address is **https://10.0.0.1.**

2. A security warning may appear. Click **Yes** or **OK** to continue. A login screen with a User Name and Password dialog boxes will display.

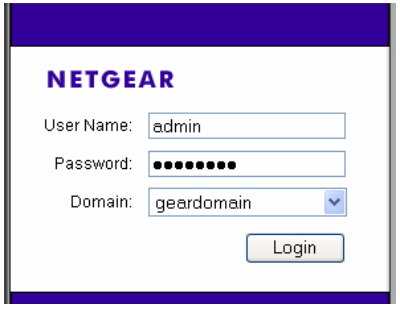

Figure 2-2

3. When prompted, enter **admin** for the User Name and **password** for the Password, both in lower case letters.
4. Select **geardomain** from the Domain drop-down menu.

5. Click **Login** to log in the **SSL VPN Concentrator** Management Interface.

   Once you have logged in, the following **Status** screen will display. The navigation links under **System Configuration, Access Administration, Monitoring, SSL VPN Portal and Web Support** menus on the left side of the browser window allow you to access and configure administrative settings. When one of the navigation options is clicked, the corresponding management configuration screen will display.

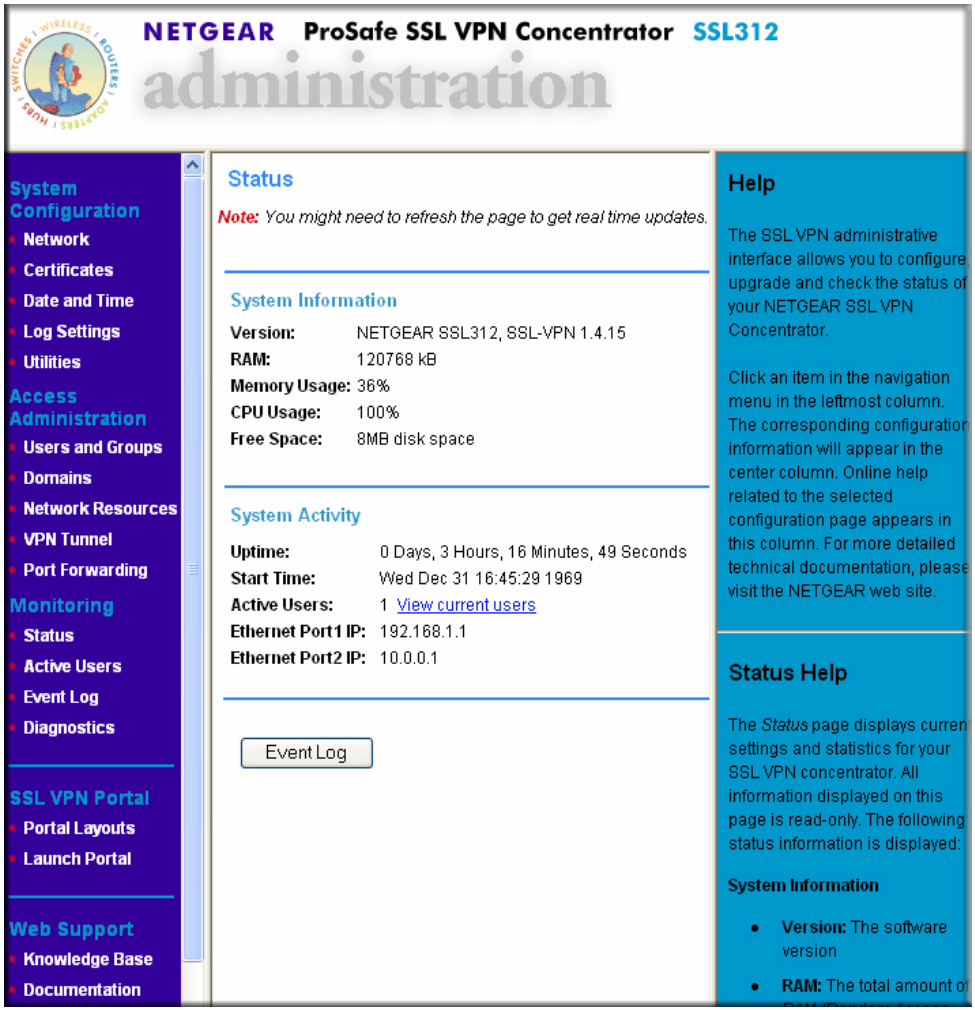

Figure 2-3

Click on the navigation links to view the corresponding management windows:

- The **Launch Portal** option under **SSL VPN Portal** in the navigation menu opens an SSL VPN portal window for users.
- In addition to the online help provided with each menu, you can access Web Support by clicking the **KnowledgeBase** link or the **Documentation** link under **Web Support** on the navigation menu.
- A **Logout** option at the bottom of the navigation menu terminates the management session and redisplays the **Login** window. If you click the **Logout** link, you must log in again in order to manage SSL VPN Concentrator.

Until an SSL certificate is uploaded to the SSL VPN Concentrator web server, the web browser may display a warning message. This message can be ignored during initial login. Please refer to "Certificate Management" in Chapter 4 on page page 4-7 for SSL certificate management instructions.

To set up the SSL VPN Concentrator you will need to:

- Configure the SSL VPN Concentrator Password, SSL certificate and general system settings (described in Chapter 4, "General Settings").
- Configure network and IP settings (Chapter 5, "Network Settings").
- Define user and group settings (Chapter 6, "Group and User Access Policies").
- Create authentication domains and portal layouts (Chapter 7, "Domains and Layouts").
- Configure network resource objects (Chapter 8, "Network Resources").
- Configure an IP address range for the VPN Tunnel client (Chapter 9, "VPN Tunnel Client").

The ProSafe SSL VPN Concentrator 25 management interface also includes System status, event logging, and log settings configuration pages (described in Chapter 3, "Status and Logging").

Once you have logged into the web user interface, an authenticated management session will be established. If you close the browser window, you must re-authenticate in order to log in into the web user interface. When you have completed the setup, you can reconfigure the computer you used for this process back to its original TCP/IP settings, if needed.

Logging in to the Management Interface

After the ProSafe SSL VPN Concentrator 25 software has been installed and the IP address configured, you may log into the ProSafe SSL VPN Concentrator 25 user interface from the web browsers listed in "Web Browser Requirements" on page 1-2. For detailed instructions on configuring the ProSafe SSL VPN Concentrator 25 software, see "Configuring the ProSafe SSL

VPN Concentrator 25". (Complete installation instructions can be found in the *ProSafe SSL VPN Concentrator 25 Installation Guide* or "Installing the SSL VPN Concentrator" on page 2-1.)

To log in to the SSL VPN Concentrator.

1. Enter the following into your web browser's Address or Location field:

   ```
   https://[IP ADDRESS/NAME OF SSL VPN Concentrator SERVER]
   ```

   A security warning may appear. Click **Yes** or **OK** to continue. A **Login** window with a Password dialogue box will display.

2. Enter the default administrator User Name and Password and select the SSL VPN Concentrator Domain to log in to the web user interface:

   - **User Name:** `[admin]`
   - **Password:** `[password]`
   - **Domain:** `[geardomain].`

   

   Note: Both the user name and password are case-sensitive.

3. Click **Login** to log in to the SSL VPN Concentrator web user interface.

Chapter 3
Status and Logging

This chapter provides an overview of the SSL VPN Concentrator administrative interface and describes the SSL VPN Concentrator status information, logging, alerting and reporting features. These settings may be viewed in the **Status and Logs** section of the SSL VPN Concentrator administrator interface.

It describes:

- SSL VPN Concentrator Status
- Event Log
- Active Users
- Log Settings

SSL VPN Concentrator Status

To view the SSL VPN Concentrator **Status** window:

1. log into SSL VPN Concentrator from a web browser using the default Ethernet Port1 IP Address, **https://192.168.1.1.**
2. Select **Status** from under the **Monitoring** menu options in the left navigation pane. The Status screen similar to the one shown below will display.

	**Note:** The status information will be unique depending upon the hardware and software configuration of the SSL VPN Concentrator server.

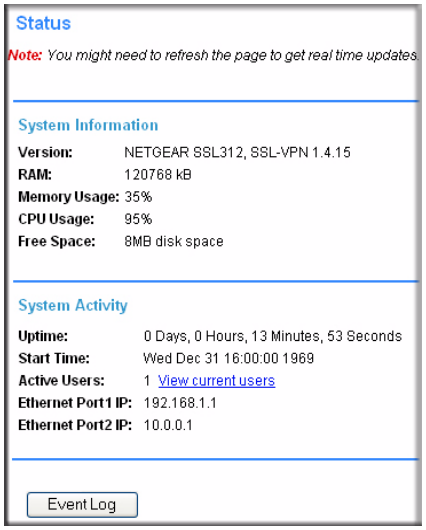

Figure 3-1

The **Status** window shows important state and configuration information. Be sure to check the **Status** window for error messages and confirm that SSL VPN Concentrator is configured properly.

From the **Status** page, you may view:

- The SSL VPN Concentrator software version
- The processor (CPU) of the SSL VPN Concentrator
- The amount of RAM memory on the SSL VPN Concentrator in MegaBytes (MB)
- The available disk space of the SSL VPN Concentrator in MegaBytes (MB)
- The uptime, the length of time since the SSL VPN Concentrator has been rebooted
- The start time, the time and date since the ProSafe SSL VPN Concentrator 25 was last started
- The number of active users. The number of active users includes administrative users. Click **View current users** or go to the **Current Users** page to view the list of current users.
- The Ethernet Port 1 and Ethernet Port 2 addresses of the SSL VPN Concentrator.

Event Log

The SSL VPN Concentrator provides web based logging. It also provides the ability to send log messages to an external syslog server using the syslog protocol and to E-mail log files and alert messages to an E-mail address or pager. To configure syslog and event log settings, see “Log Settings” on page 3-6.

To view the SSL VPN Concentrator event log:

Click **Event Log** under the Monitoring menu in the left navigation menu. The **Event Log** window displays.

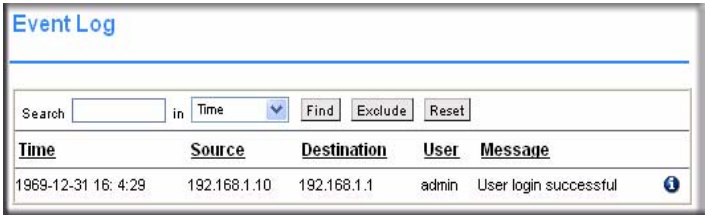

Figure 3-2

The **Event Log** window displays log messages in a sortable, searchable table. The SSL VPN Concentrator stores 250Kb of log data or approximately one thousand log messages. Once the log file reaches the log size limit, the log is cleared and, optionally, e-mailed to the SSL VPN Concentrator administrator.

Each event log entry displays the following information (if applicable):

- **Time and date of log event.** The time stamp displays the date and time of log events. The time and date is displayed as “Year-Month-Day Hour:Minute:Second”. Hours are displayed in 24-hour clock format, so 2:00 PM is displayed as hour 14 in the event log. The date and time are based on the local time of the SSL VPN Concentrator, which is configured on the **Date and Time** screen under the **System Configuration** menu.
- **Source address**. The Source IP address shows the IP address of the user or administrator that generated the log event. The source IP address may not be displayed for certain events, such as system errors.
- **Destination address**. The destination IP address field shows the name or IP address that received the event. For example, if a user accessed an Intranet web site through the SSL VPN portal, the corresponding log entry would display the IP address or fully qualified domain name of the web site accessed.

- **User name**. The User name field shows the authenticated name of the user or administrator that generated the log event.
- **Log message**. The message field describes the event that occurred. Examples of log messages include "`Administrator login successful`" and "`SSL VPN Concentrator restarting`".
- **Log priority**. The priority of log messages are divided into seven categories:

Table 3-1. Priority of Log Messages

Value	Definition
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Information
7	Debug

The event log table may be sorted and filtered.

To sort the event log by category:

1. Click the category header to be sorted, such as **Time** or **Source**.
2. Enter the search term in the **Search** field.
3. Select an event category from the pull-down menu and click **Find**.

To filter messages:

1. Enter the term to be filtered in the **Search** field.
2. Select the event category from the pull-down menu and click **Exclude**.

To reset the search results and display all log messages, click **Reset**.

Note: The **Find** and **Exclude** search tools are both case sensitive

By default, 50 messages are displayed per page. If more than 50 events have been logged, then a **Page** number menu will be displayed at the top of the event log table. Select the desired page number from the **Page** menu to see archived log messages.

On the **Log Settings** page, you can configure the type of messages, such as warning and alert messages, that will be displayed in the event log. You can also configure log rotate features on the **Log Settings** page which will determine when to clear the log files.

Active Users

The **Active Users** screen displays the active users and administrators logged into the SSL VPN portal.

To view the Active Users log file, click **Active Users** under the Monitoring menu in the left navigation pane.

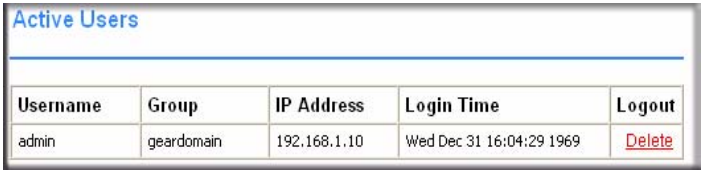

Figure 3-3

The **Active Users** window displays the current users or administrators logged into the SSL VPN Portal or the SSL VPN Concentrator administrative interface. Each entry displays the name of the user, the group in which the user belongs, the IP address of the user and a time stamp indicating when the user logged in.

A user will continue to appear in the **Active Users** table until the user manually logs out of the SSL VPN Portal or until an inactivity timeout occurs. Consequently, some users may appear in the **Active Users** table for several minutes after they have closed their browser windows.

An administrator may terminate a user session and log the user out by clicking the **Delete** link in the **Logout** column adjacent to the user.

Log Settings

The SSL VPN Concentrator supports web-based logging, syslog logging and e-mail alert messages. In addition, the SSL VPN Concentrator may be configured to e-mail the event log file to the SSL VPN Concentrator administrator before the log file is cleared.

Syslog is an industry-standard logging protocol that records system and networking activity. The SSL VPN Concentrator syslog messages are sent in WELF (WebTrends Enhanced Log Format), so most standard firewall and networking reporting products can accept and interpret the SSL VPN Concentrator log files. The SSL VPN Concentrator syslog service transmits syslog messages to external syslog server(s) listening on UDP port 514.

To configure **Syslog Settings**, **E-mail Settings** and **Log and Alert Categories** for syslog and alert settings:

1. Click **Log Settings** under the System Configuration menu in the left navigation pane.

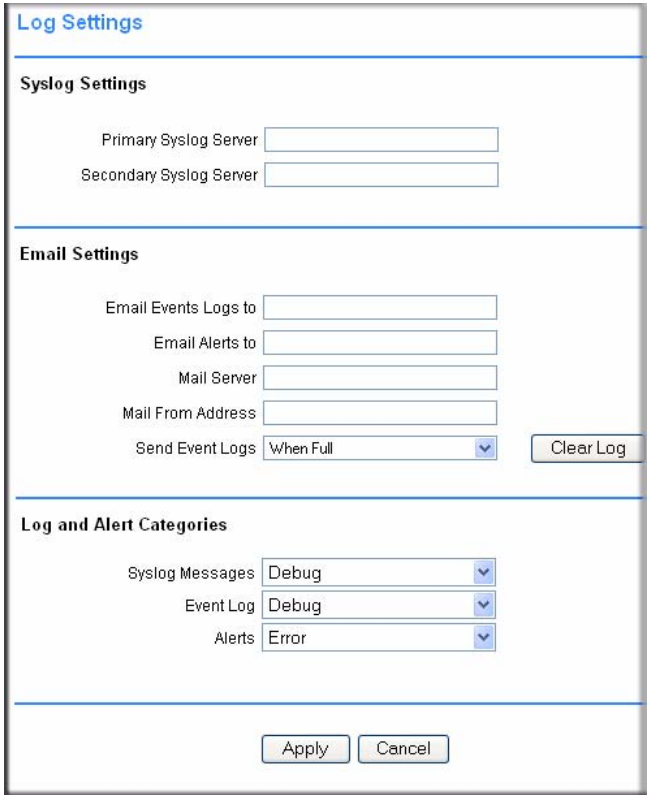

Figure 3-4

2. In the **SysLog Settings** section, enter the IP address or fully qualified domain name of your syslog server in the **Primary Syslog Server** field. Leave this field blank if you do not require syslog logging.
3. If you have a backup or second syslog server, enter the IP address or domain name of the Secondary Syslog Server in the **Secondary Syslog Server** field.
4. In the **E-mail Settings** section:
   a. Enter your full e-mail address (username@domain.com) in the **E-mail Event Logs to** field to receive e-mail notification. The event log file will be e-mailed to the specified e-mail address before the event log is cleared. If this field is left blank, log files will not be e-mailed.
   b. Enter your full e-mail address (username@domain.com) or an e-mail pager address in the **E-mail Alerts** to field to receive alert messages via e-mail. An e-mail will be sent to the e-mail address specified if an alert event occurs.
   c. Enter the name or IP address of your mail server in the **Mail Server** field to e-mail log files or alert messages. If this field is left blank, log files and alert messages will not be e-mailed.
   d. Enter the e-mail address that log and alert messages will be e-mailed from in the **Mail From Address** field.
   e. Configure how frequently log files will be e-mailed and cleared in the **Send Event Logs** field. If the option “When Full” is selected, the event log will be e-mailed and then cleared when the log file is full. If “Daily” or “Weekly” options are selected, then
      - The log file will be e-mailed and deleted on a daily or weekly basis.
      - The log file will still be cleared if the log file is full before the end of the period
   f. From the **Send Event Logs** pull-down menu, select a schedule for sending Event Logs. You can also manually clear the Event Logs by clicking **Clear Log.**
5. In the **Log and Alert Categories** section, define the type of events that will generate Syslog Messages, Event Logs and Alert messages from the **Syslog Messages, Event Log** and **Alerts** pull-down menus.

   Log categories are organized from most to least critical. Once a category is selected, then all events equal to or more critical than the selected log category and will be logged. The default Log and Alert categories are:

   - Syslog Messages: Debug
   - Event Log: Debug

- Alerts: Error

6. Click **Apply** to confirm your settings.

Chapter 4
General Settings

This chapter provides instructions for saving and restoring the configuration file, upgrading the firmware and for managing SSL certificate files. It also covers restarting the SSL VPN Concentrator and configuring the time and date settings. Sections include:

- Exporting and Saving a Backup Configuration File
- Importing a Configuration File
- Erasing and Restoring the Default Settings
- Upgrading the SSL VPN Concentrator Firmware
- Time and Date Settings
- Certificate Management

System Configuration Utilities

The **Utilities** window allows you to export the SSL VPN Concentrator configuration file, import a saved configuration file, upgrade the SSL VPN Concentrator software, restore the settings to factory defaults and restart the SSL VPN Concentrator server. In addition, it allows users to import and encrypt the configuration files.

To access the SSL VPN Concentrator software and system settings, click **Utilities** under the System Configuration menu in the left navigation page. The **Utilities** screen shown below will display.

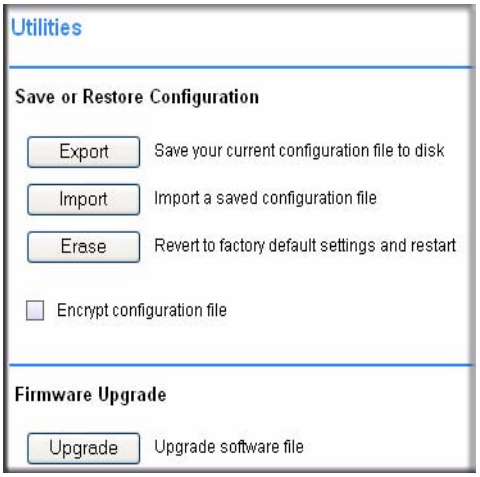

Figure 4-1

Encrypting the Configuration File

For security purposes, you can encrypt the configuration files. However, if the configuration files are encrypted, they cannot be edited or reviewed for troubleshooting purposes.

To encrypt the configuration files:

Check the **Encrypt configuration** file radio box. The Configuration files will be encrypted when they are exported to disk.

Exporting and Saving a Backup Configuration File

You may save the SSL VPN Concentrator configuration settings to a backup file and then import the saved configuration file later.

To save a backup version of theSSL VPN Concentrator configuration:

1. From the **Save or Restore Configuration** section, click **Export**.
2. A screen similar to the one shown below will display prompting you to Open or Save the file. Click **Save**.

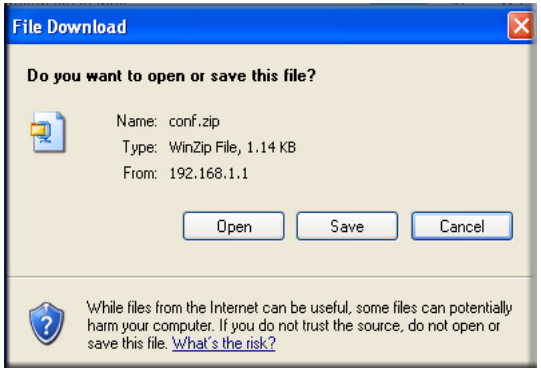

Figure 4-2

3. Choose the location to save the configuration file. The file is named “conf.zip” by default, but it can be renamed.
4. Click **Save** to save the configuration file.

Importing a Configuration File

To import a saved configuration file:

1. Click **Import**. A window similar to the following will display.

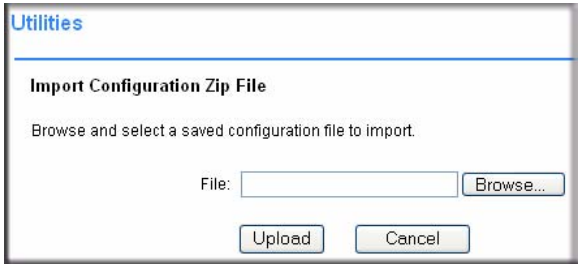

Figure 4-3

2. Click **Browse** to locate a saved configuration zip file. The configuration zip file should contain the `gearhost.conf`, `smm.conf` and `tunneld.conf` files.
3. Select the file and then click **Import**.
4. Restart the SSL VPN Concentrator server for the settings changes to take effect.

Erasing and Restoring the Default Settings

To erase your SSL VPN Concentrator configuration settings and restore the initial configuration:

1. Click **Erase**.
2. A dialog box will prompt you to confirm the change. Click **OK** to restore the initial configuration settings.

Figure 4-4

The SSL VPN Concentrator software will automatically be restarted and all active connections will be dropped.

	Note: The IP address settings are not reset.

Upgrading the SSL VPN Concentrator Firmware

	Note: Be sure to export the SSL VPN Concentrator configuration file before upgrading the firmware in case the software is corrupted or the entire system needs to be reinstalled.

To install a new version of the SSL VPN Concentrator firmware:

1. Click **Upgrade**. A window similar to the following will display.

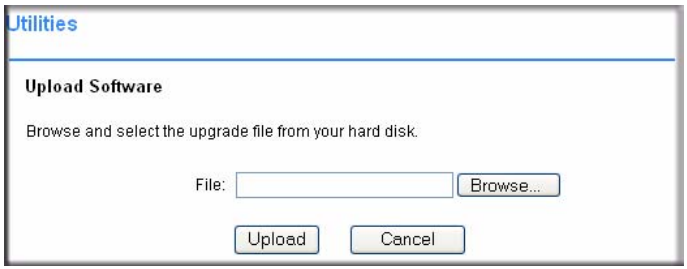

Figure 4-5

2. Click **Browse** to locate the saved firmware file, `ssl312-X.X.X.tar.gz`, where *X.X.X* indicates the release version.
3. Select the file and then click **Upload**.
4. Once the file has been uploaded, restart the SSL VPN Concentrator server for the upgrade to be complete.

Time and Date Settings

To configure the SSL VPN Concentrator time and date settings:

1. Click **Date and Time** under the System Configuration menu in the left navigation pane.

   The SSL VPN Concentrator uses the time and date settings to timestamp log events and for other internal purposes.

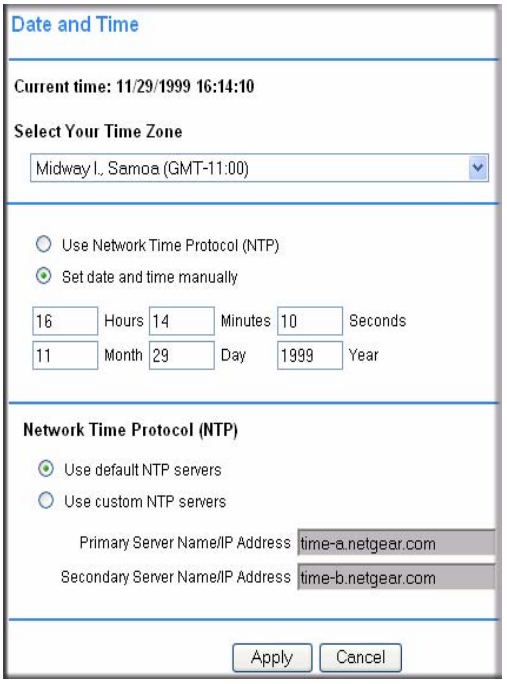

Figure 4-6

2. Select your time zone from the **Select Your Time Zone** drop-down menu.
3. Select either the **Use Network Time Protocol (NTP)** radio box or the **Set date and time manually** radio box. If you selected the manual option, enter the desired time (in 24-hour time format) in the Hours, Minutes, Seconds, Month, Day and Year fields.
4. Select the **Network Time Protocol (NTP)** to be used.
   - If you selected the **Use default NTP servers** radio button, the default primary and secondary servers will be selected.
   - If you selected the **Use custom NTP servers,** enter an NTP server IP address or fully-qualified domain name (FQDN) in the address fields. (For redundancy, enter a backup custom server address in the **Secondary Server Name/IP Address** field.)
5. Enter the address of your primary and secondary servers in the **Primary Server Name/IP Address** and **Secondary Server Name/IP Address** fields. (The defaults are time-zone specific.)
6. Click **Apply** to update the configuration.

If you enabled NTP, then the NTP time settings will override the manually configured time settings. The NTP time settings will be determined by the NTP server and the time zone that is selected in the **Select Your Time Zone** menu.

Certificate Management

In order to get a valid certificate from a widely accepted Certificate Authority such as Verisign or Thawte, you must generate a Certificate Signing Request (CSR) for your SSL VPN device.

From the **Certificates** window, you can view the currently loaded certificates, upload a digital certificate and generate a new Certificate Signing Request (CSR).

To generate a new Certificate Signing Request (CSR) file:

1. Under the System Configuration menu in the left navigation pane, select **Certificates**. The **Certificates** screen will display.

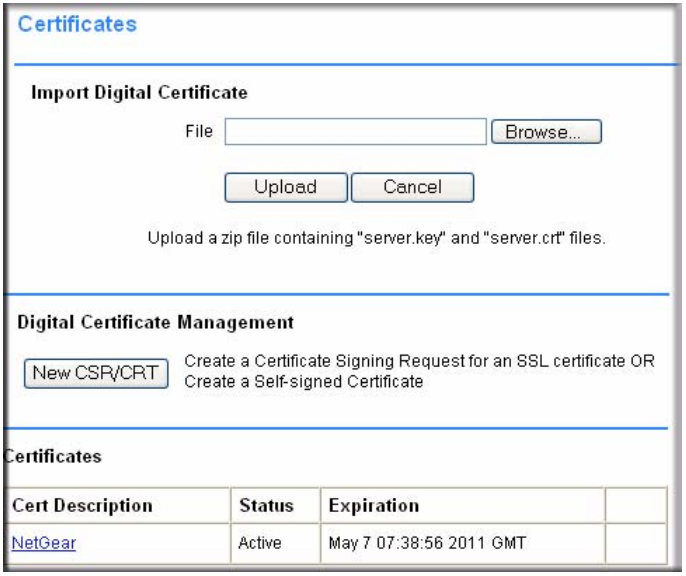

Figure 4-7

2. Click **New CSR/CRT** in the **Digital Certificate Management** section. The **Create CSR** screen will display.

3. Fill out all of the fields with the appropriate information.

Figure 4-8

4. Check the **Generate a Self-signed Certificate** radio box to generate a new CRT.

   If all information is entered correctly, a crt.zip file will be created. This file includes a server.crt and a server.key key file. You will need to provide these files to the Certificate Authority.

	Note: Do not directly upload the CSR to SSL VPN Concentrator.

5. Click **Apply.** A file Download screen will display. Click **Save** to save the csr.zip file to a disk location.
6. Click **Back** to return to the **Certificates** screen.
7. In the **Import Digital Certificate** table, select **Browse** to locate the zipped digital certificate file on your disk or network drive. Any file name will be accepted, but it must have the "`.zip`" extension. The zipped file should contain a certificate file named "`server.crt`"

and a certificate key file named "`server.key`". If the zipped file does not contain these two files, the zipped file will not be uploaded

8. Click **Upload** to save the file to the **Cert Description** table. Once the certificate has been uploaded, the certificate will be displayed in the **Current Certificates** table

> **Note:** Valid certificates generated by an authorized Certificate Authority (CA) require a password. Before you enable the certificate and restart the software, be sure to enter the correct certificate password on the **View Certificate** window.

To activate the newly uploaded certificate:

1. Select the **Enable** radio button adjacent to the new certificate. The **Enable Certificate** screen will display.

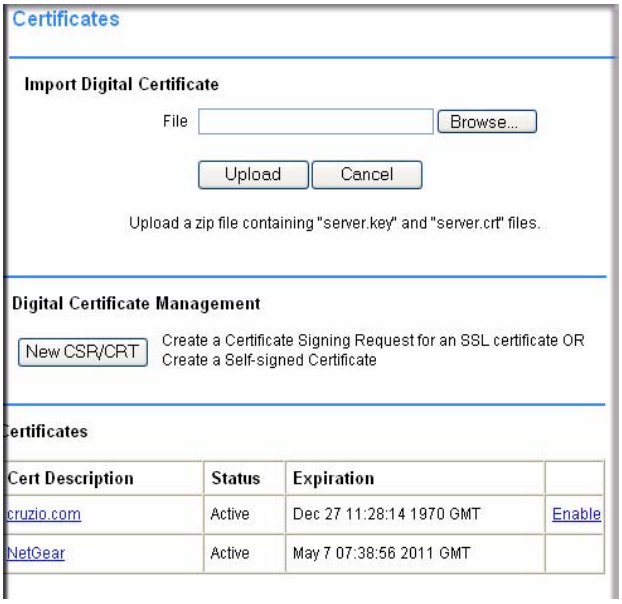

Figure 4-9

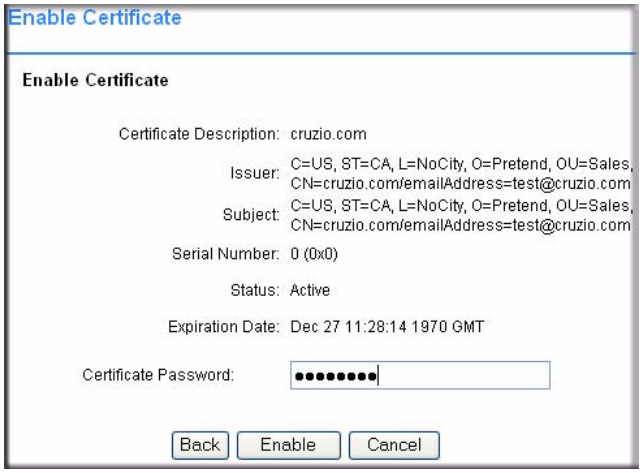

Figure 4-10

2. Click **Enable**. The SSL VPN Concentrator software will restart using the new certificate.

In order to obtain a valid certificate from a widely accepted Certificate Authority such as Verisign or Thawte, you must generate a Certificate Signing Request for your SSL VPN device.

	Note: Most valid certificates created by a Certificate Authority (CA) require a password. Before you enable the certificate and restart the software, be sure to enter the correct certificate password on the **View Certificate** screen.

The **Current Certificates** table lists the valid SSL certificates. (The Certificate being used by the SSL VPN Concentrator will not show an “enable” link.)

To view details of currently available certificates:

In the **Certificate** table, click the name of the certificate. The **View Certificate** window will display for that certificate From the **View Certificate** window, you can view the issuer and certificate subject information.

Figure 4-11

You may also delete an expired or incorrect certificate. Delete the certificate by clicking **Delete** .

	Note: The Delete button will not be displayed if the SSL certificate is active. To delete a certificate, upload and activate another SSL certificate. Then you can delete the inactive certificate from the View Certificate window.

Chapter 5
Network Settings

This chapter describes how to configure network and IP settings. These settings should be configured by a network administrator. The Network settings to be configured include:

Configuring Network Settings

The IP settings and interface settings of the SSL VPN Concentrator appliance may be configured through the **Network** screen under the System Configuration menu on the left navigation panel. From the **Network** window, an SSL VPN Concentrator administrator can

- Set the Ethernet Port 1 and Ethernet Port 2 addresses.
- Define the default network route and add additional static IP routes.
- Map host names or fully qualified domain names to IP addresses.
- Manage SSL Certificates (as described in "Certificate Management" in Chapter 4).

Warning: These advanced network settings should only be configured by a network administrator.

Sample SSL VPN Concentrator Configuration

In the following network configuration example, the SSL VPN Concentrator appliance is deployed as a standalone SSL VPN device. A separate access router or firewall performs perimeter security.

- **Interface Ethernet Port 1 IP address:** `192.168.1.1`

- **Interface Ethernet Port 1 subnet mask:** `255.255.255.0` (subnet: `192.168.1.0/24`)
- **Default gateway address (Firewall/Router address):** `192.168.1.2`

In this configuration, the IP addresses of devices in the local network should be configured in the `192.168.1.0/24` subnet and the default gateway for these devices should be the internal IP address of the local firewall or router, `192.168.1.2`. A network diagram of this configuration is displayed below.

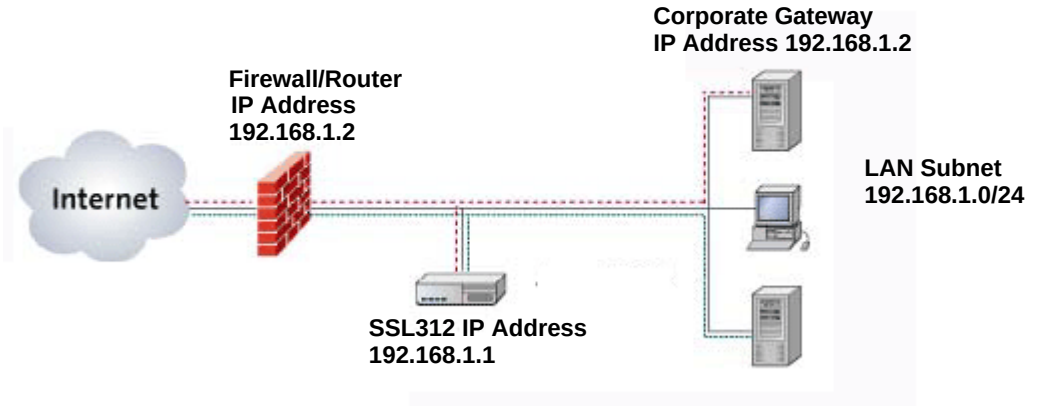

Figure 5-1

All connections initiated from the Internet can be blocked by the firewall except HTTPS traffic (TCP port 443). HTTPS traffic should be forwarded to the SSL VPN Concentrator appliance address, `192.168.1.1`.

Network Interface Configuration

Configure the SSL VPN Concentrator network **Interface** settings by selecting **Network** under the System Configuration menu in the left navigation pane and then clicking the **Interface** radio button.

To configure the Ethernet Port 1 and Ethernet Port 2 Interfaces:

1. Enter the Ethernet Port 1 (SSL) IP address of your SSL VPN Concentrator. This address should be a unique address in the same subnet as the rest of your local network. The factory default is 192.168.1.1.

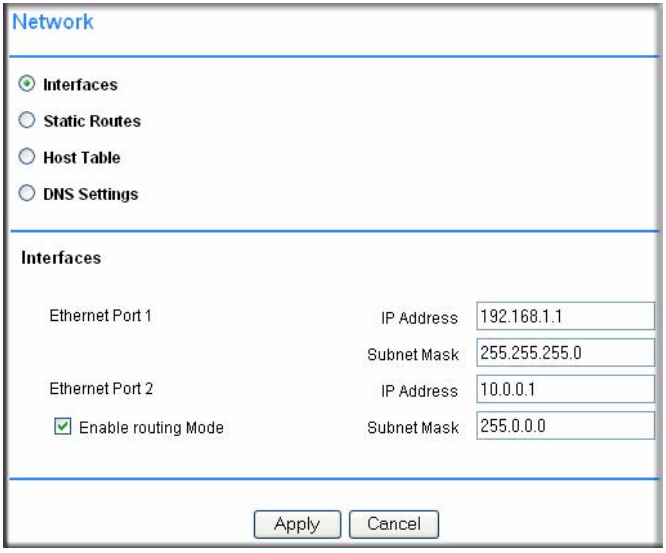

Figure 5-2

2. Enter the Ethernet Port 1 subnet mask that has been configured for your network. The subnet mask value should be the same value as the subnet mask configured on your network computers. The factory default is 255.255.255.0 (The subnet mask specifies the network number portion of an IP address.).
3. **Enable two port operation** by checking this radio box. A second Ethernet port will be enabled.

	Note: One port operation is recommended for most networks.

4. Enter a local or internal IP address of your ProSafe SSL VPN Concentrator 25. This address should be in a different subnet than the Ethernet Port 1 IP address. The default Ethernet Port 2 IP Address is 10.0.0.1.
5. Enter the subnet mask. The subnet mask specifies the network number portion of an IP address. The factory default is 255.255.255.0.

6. Click **Apply** to save your settings.

	**Note:** The SSL VPN Concentrator does not perform Network Address Translation (NAT). And the SSL VPN Concentrator only enforces access policies on SSL VPN traffic, not on other TCP/IP protocols. Therefore, the SSL VPN Concentrator should be used in conjunction with a network firewall.

If the interface is configured to terminate SSL VPN connections, then restart the SSL VPN Concentrator software for the change to take effect.

	**Note:** The SSL VPN Concentrator administrative session will end when the software is restarted. To log in to the SSL VPN Concentrator management interface, enter the new IP address of the SSL VPN Concentrator device in the Address or Location field of your web browser. Be sure that the management station is in the same subnet as the new SSL VPN Concentrator IP address.

To complete the IP settings configuration, also configure SSL VPN Concentrator DNS settings and network routes.

Network Route Configuration

From the Network Route screen, you can define the default network route and add additional static routes to local area subnets. **The default route is required for Internet access**; static routes are optional.

To configure the default route:

1. Check the **Static Routes** radio button on the **Network** screen. The **Network** screen will display both **Add Default Route** and **Add Static Routes** fields, as shown below.
2. In the **Add Default Route** section, enter the IP address of the router or default gateway of the network in the **Default Gateway Address** field.

   The default gateway address is the same gateway address used by local area network computers to connect to the Internet and it may be the address of a network firewall.
3. Select the Ethernet interface (ethernet-1 or ethernet-2) that should be used to connect to the default gateway address from the **Interface** pull-down menu.
4. Click **Apply**. Once updated, the route will be displayed in the **Static Routes** table.

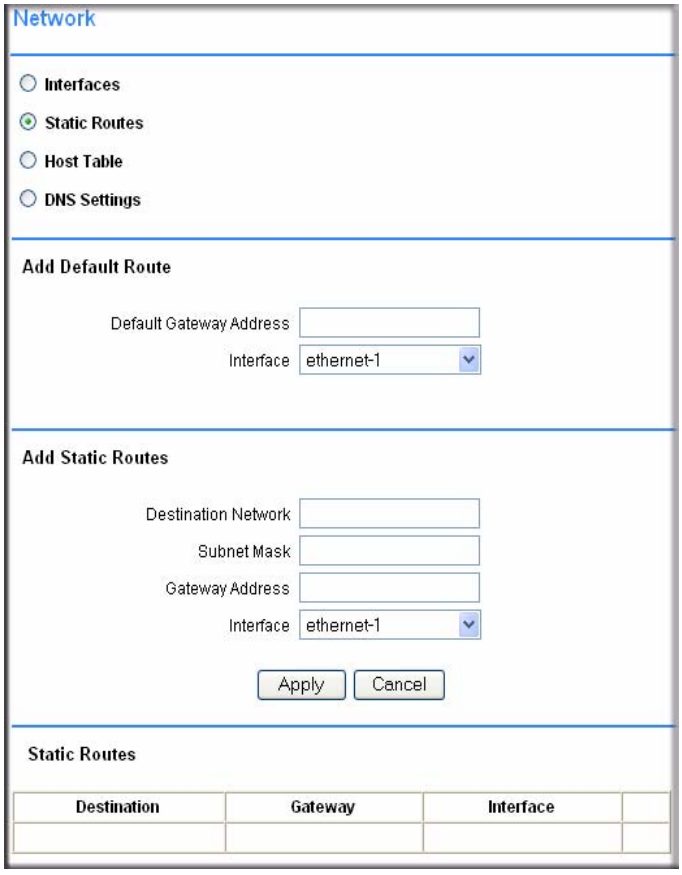

Figure 5-3

To configure a static route:

1. In the **Add Static Routes** section, enter the destination network address of the static route in the **Destination Network** field. The destination network address is an IP address in the remote network subnet.

> **Note:** The destination network address may be a valid IP address or it may be a subnet address that ends in ".0", such as "192.168.0.0".

2. Enter the subnet mask of the remote network segment in the **Subnet Mask** field.

3. Enter the IP address of your router in the **Gateway Address** field. The gateway address should be in the same subnet as the ethernet-1 or ethernet-2 interface.

   For example, if the ethernet-1 interface address is "`10.0.0.100`" and the subnet mask is "`255.255.255.0`", then a router connected through the ethernet-1 interface should be "`10.0.0.X`".

4. Select the Ethernet interface that should be used to connect to the gateway address from the **Interface** menu (ethernet-1 or ethernet-2).

5. Click **Apply**. Once the domain has been added, the domain will be added to the **Routes** table.

> **Note:** To add additional local subnets that can directly connect to the ProSafe SSL VPN Concentrator 25 device, define the **Destination Network** address, the **Subnet Mask**, and the **Interface**, but leave the **Gateway Address** field blank.

Network Host Table Settings

From the **Host Table** screen you can map host names or fully qualified domain names (FQDNs) to IP addresses.

> **Note:** The SSL VPN Concentrator can act as a NetBIOS and a WINS (Windows Internet Naming Service) client to learn local network host names and corresponding IP addresses.

To configure host resolution:

1. Check the **Host Table** radio button on the **Network** screen. The **Network** screen will display the **Add Host** fields and the **Host Table**.

2. Enter the IP Address of the machine that will be mapped to a host name in the **IP Address** field.

3. Enter the host name or Fully Qualified Domain Name of the machine in the **Host Name** field. For example, enter "mycomputer" or "www.netgear.com". Do not enter names with spaces or other non-ASCII characters such as apostrophes or commas.

4. Enter the host alias in the optional **Alias** field. For example, if a FQDN "www.netgear.com" has been entered in the **Host Name** field, then a shorter name, such as "www" or "web" may be entered in the **Alias** field.

5. Click **Apply**.

Once the new Host has been added, the Host will be displayed in the **Host Table.** The **Host Table** displays a list of the configured host names and the corresponding IP addresses

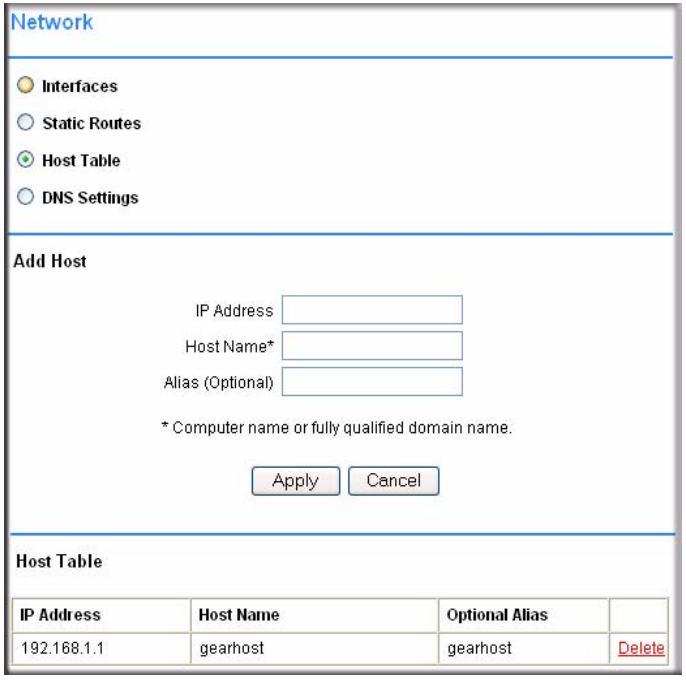

Figure 5-4

Configuring DNS Settings

The DNS Settings window allows the ProSafe SSL VPN Concentrator 25 administrator to configure the hostname, DNS server addresses and WINS server addresses. The WINS server configuration is optional; the DNS server configuration is required.

To configure the ProSafe SSL VPN Concentrator 25 hostname, DNS settings and WINS settings:

1. Check the **DNS Settings** radio box on the **Network** screen. The **Network** screen will display the fields for entering the **DNS Settings.**

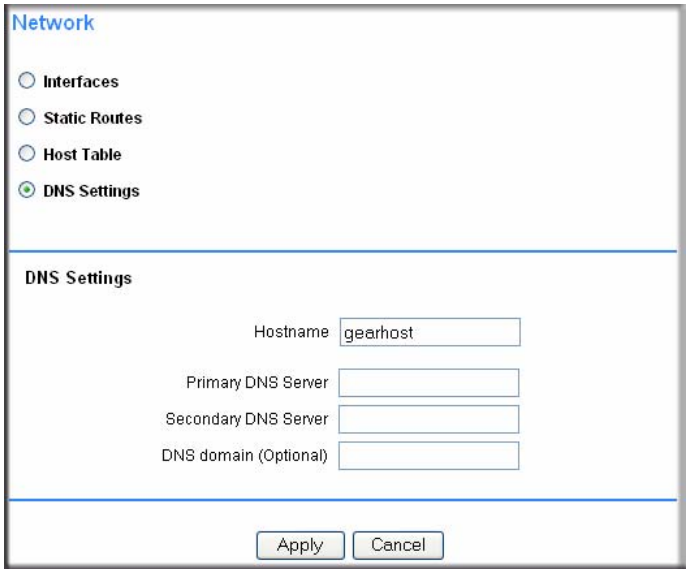

Figure 5-5

2. Enter the **Hostname** for the ProSafe SSL VPN Concentrator 25 device. The hostname is used to identify the SSL VPN Concentrator device on the network. Use only letters and numbers for the hostname; do not enter non-ASCII characters such as spaces or apostrophes.
3. Enter the IP address of your DNS server in the **Primary DNS Server** field.
4. For redundancy, enter the IP address of a backup DNS server in the **Secondary DNS Server** field.
5. Enter the domain name of your network in the **DNS Domain** field. This field is optional and is not required for most network environments.
6. Click **Apply** to update the configuration.

	Note: If you update the SSL VPN gearhost hostname, you must restart the ProSafe SSL VPN Concentrator 25 software for the change to take effect. DNS settings changes take effect immediately.

Chapter 6
Group and User Access Policies

This chapter describes how to define users and groups and how to configure SSL VPN Concentrator access policies and bookmarks for the users and groups. This chapter includes the following topics:

- Editing Global Policy Settings
- Adding and Editing Global Policies
- Defining and Editing Global Bookmarkss
- Adding a New Group, Deleting a Group and Editing Group Settings
- Defining and Editing Group Policies
- Defining and Editing Group Bookmarks
- Adding a New User, Deleting a User and Editing a User
- Defining and Editing User Policies
- Defining and Editing a User Bookmarks
- Active Directory Authentication Servers for Group Policies and Bookmarks
- LDAP Authentication Domains for Group Policies and Bookmarks
- NT and RADIUS Domain Servers for Group Policies and Bookmarks

Users, Groups and Global Policies

An administrator can define user, group and global policies to predefined network resource objects, IP addresses, address ranges, or all IP addresses and to different SSL VPN services. A specific hierarchy is invoked over which policies take precedence. The SSL VPN Concentrator policy hierarchy is defined as:

1. **User Policies** take precedence over all **Group Policies**.
2. **Group Policies** take precedence over all **Global Policies**.

3. If two or more user, group or global policies are configured, the ***most specific policy takes precedence***.

For example, a policy configured for a single IP address takes precedence over a policy configured for a range of addresses. And a policy that applies to a range of IP addresses takes precedence over a policy applied to all IP addresses. If two or more IP address ranges are configured, then the smallest address range takes precedence. Hostnames are treated the same as individual IP addresses

Network Resources are prioritized just like other address ranges. However, the prioritization is based on the individual address or address range, not the entire Network Resource.

For example, let's assume the following global policy configuration:

- **Policy 1:** A Deny rule has been configured to block all services to the IP address range `10.0.0.0 - 10.0.0.255`.
- **Policy 2:** A Deny rule has been configured to block FTP access to `10.0.1.2 - 10.0.1.10`.
- **Policy 3:** A Permit rule has been configured to allow FTP access to the predefined network resource, **FTP Servers**. The **FTP Servers** network resource includes the following addresses:`10.0.0.5 - 10.0.0.20` and `ftp.company.com`, which resolves to `10.0.1.3`.

Assuming that no conflicting user or group policies have been configured, if a user attempted to access:

- An FTP server at `10.0.0.1`, the user would be blocked by **Policy 1**.
- An FTP server at `10.0.1.5`, the user would be blocked by **Policy 2**.
- An FTP server at `10.0.0.10`, the user would be granted access by **Policy 3**. The IP address range `10.0.0.5 - 10.0.0.20` is more specific than the IP address range defined in **Policy 1**.
- An FTP server at ftp.company.com, the user would be granted access by **Policy 3**. A single host name is more specific than the IP address range configured in **Policy 2**.

Note: The user would not be able to access ftp.company.com using its IP address 10.0.1.3. The SSL VPN Concentrator policy engine does not perform reverse DNS lookups.

Global Policies

You can view and configure the SSL VPN Concentrator Global Policies, Groups and Users by selecting **Users and Groups** under the Access Administration menu in the left navigation pane.

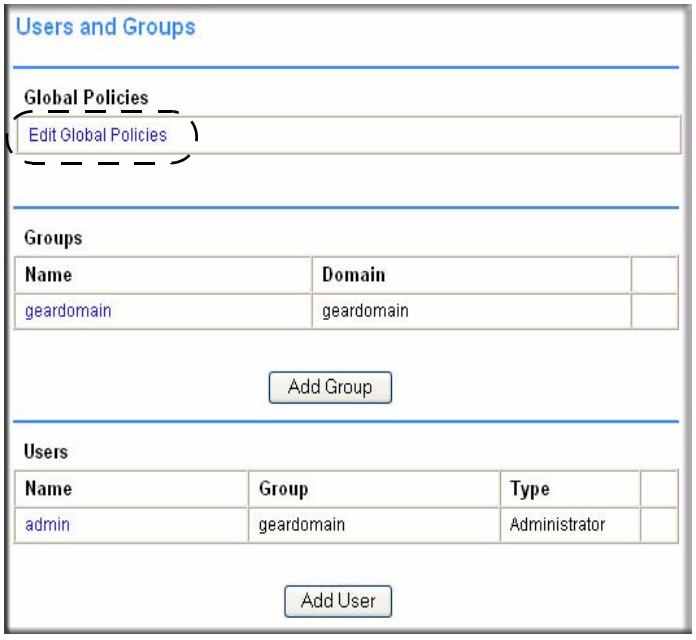

Figure 6-1

Editing Global Policy Settings

To edit global settings:

1. Click the **Edit Global Policies** link in the **Global Policies** table. The **Global Settings** screen will display.

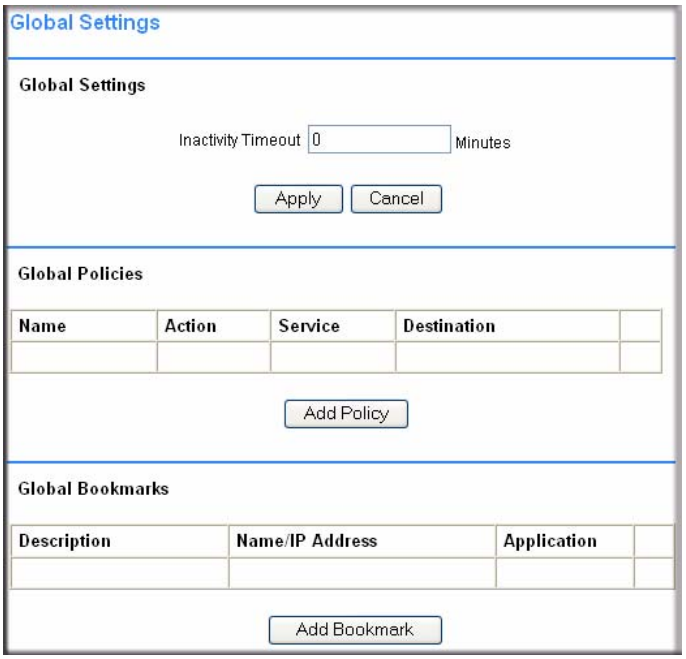

Figure 6-2

2. Enter the number of minutes of inactivity to allow in the **Inactivity Timeout** field.
3. Click **Apply** to save the configuration changes.

   The inactivity timeout can be set at the user, group and global level. If one or more timeouts are configured for an individual user, the user timeout setting will take precedence over the group timeout and the group timeout will take precedence over the global timeout.

   Setting the global settings timeout to 0 disables the inactivity timeout for users that do not have a group or user timeout configured.

Adding and Editing Global Policies

To define global access policies:

1. Click **Add Policy** in the **Global Policies** section. An **Add Policy** window will be displayed.

	Note: User and group access policies will take precedence over global policies.

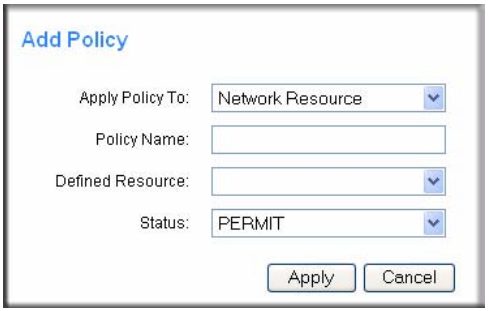

Figure 6-3

2. From the **Apply Policy To** pull-down menu, select whether the policy will be applied to a predefined network resource, an individual host, a network or all addresses.
3. Enter a name for the policy in the **Policy Name** field.

> **Note:** SSL VPN Concentrator policies apply to the destination address(es) of the SSL VPN connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the SSL VPN Concentrator through the policy engine.

   - If your policy applies to a predefined network resource, select the name of the resource from the **Defined Resource** menu. For information about creating network resources, refer to Chapter 8, "Network Resources".
   - If your policy applies to a specific host, enter the IP address of the local host machine in the **IP Address** field.
   - If your policy applies to a network, enter the network address in the **Network Address** field and the subnet mask in the **Subnet Mask** field.
4. Select the service type from the **Service** pull-down menu. If you are applying a policy to a network resource, the service type is defined in the network resource.
5. Select **PERMIT** or **DENY** from the **Status** pull-down menu to either permit or deny SSL VPN connections for the specified service and host machine.
6. Click **Apply** to update the configuration. Once the configuration has been updated, the new policy will be displayed in the **Global Policies** table on the **Global Settings** screen.

   The Global Policies will be displayed in the order of priority, from the highest priority policy to the lowest priority policy.

Defining and Editing Global Bookmarks

To define global bookmarks:

1. Click **Add Bookmark** in the **Global Bookmarks** section. An **Add Bookmark** window will be displayed.

Figure 6-4

When global bookmarks are defined, all members will see the defined bookmarks from the SSL VPN portal. Individual users will not be able to delete or modify global bookmarks.

2. Enter a descriptive name in the **Bookmark Name** field.
3. Enter the domain name or the IP address of a host machine on the LAN in the **Name or IP Address** field.
4. Select the service type from the **Service** pull-down menu
5. Select the screen size for viewing bookmark data from the **Screen Size** pull-down menu.
6. Click **Apply** to update the configuration. Once the configuration has been updated, the new global bookmark will be displayed in the **Global Bookmarks** table on the **Global Settings** screen.

Groups Configuration

When configuring Groups, remember that user policies take precedence over all group policies and group policies take precedence over all global policies, regardless of the policy definition. (A user policy that allows access to all IP addresses will take precedence over a group policy that denies access to a single IP address).

SSL VPN Concentrator Groups are also defined from the **Users and Groups** screen. Select the **Users and Groups** option under the **Access and Administration** menu in the left navigation pane. The **Users and Groups** screen will display

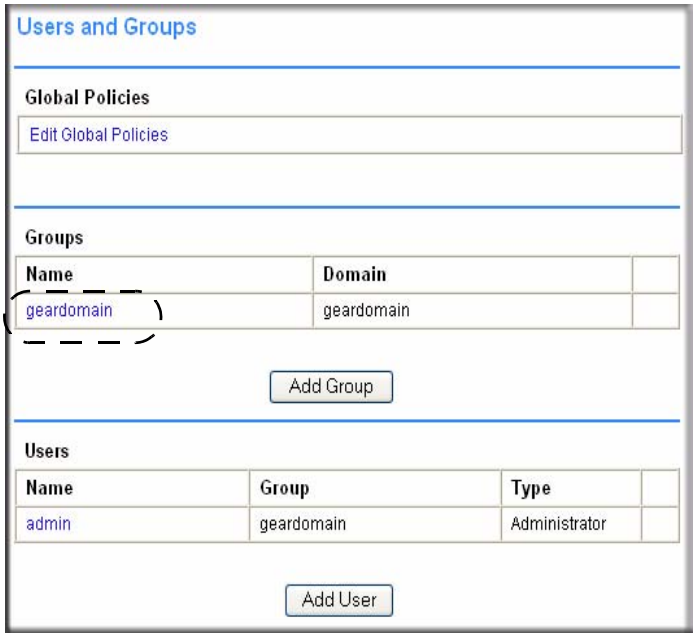

Figure 6-5

Adding a New Group

To create a new group:

1. Click **Add Group** on the **Users and Groups** screen (see Figure 6-2). An **Add Group** window will display.

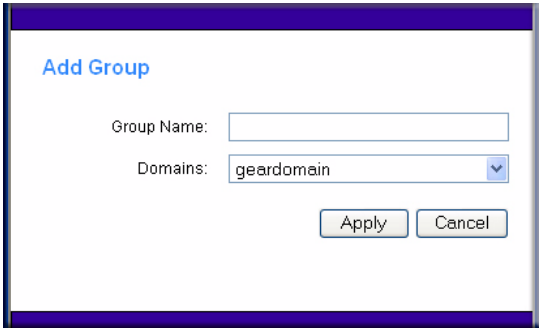

Figure 6-6

2. Enter a descriptive name for the group in the **Group Name** field.
3. Select the appropriate domain in the **Domain** menu. The domain will determine the authentication method for the group.
4. Click **Apply** to update the configuration. Once the group has been added, the new group will be added to the **Groups** table on the **User and Groups** screen.

   All of the configured groups are displayed in the table on the **Users and Groups** screen. The Groups are listed in alphabetical order.

Editing Group Settings

To edit group settings:

1. Click the name of the group in the **Groups** table. The **Edit Group Settings** window will display. The general group information, including the **Group Name**, **Domain Name**, and **Inactivity Timeout** will be displayed. The **Group Name** and **Domain Name** are not configurable.
2. Set the inactivity timeout for users in the group by entering the number of minutes of inactivity to allow in the **Inactivity Timeout** field.
3. Click **Apply** to save the configuration changes.

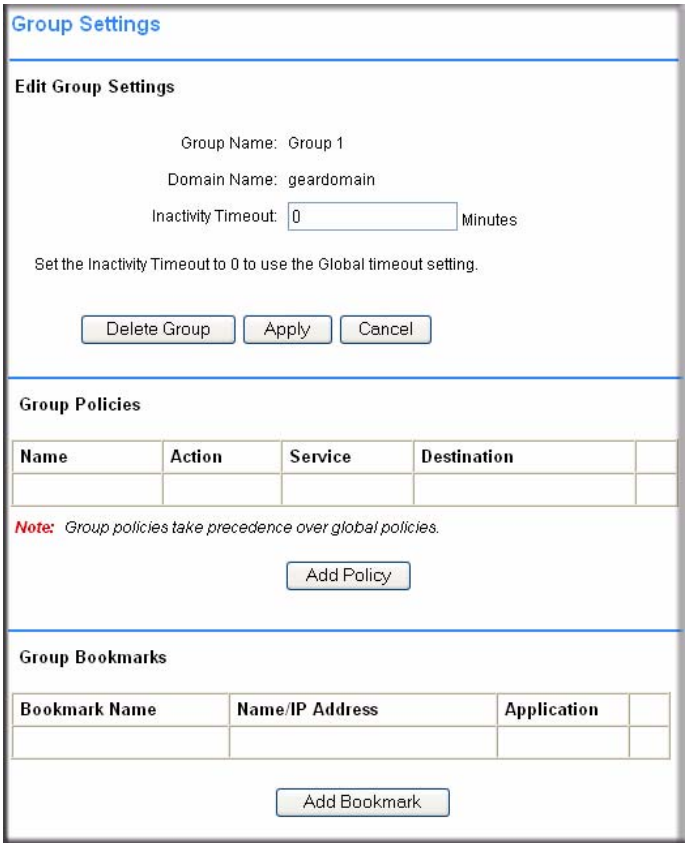

Figure 6-7

The inactivity timeout can be set at the user, group and global level. Set the timeout as 0 in the user and group configuration to use the global timeout setting. If multiple timeout settings are configured, the user timeout setting will take precedence over the group timeout and the group timeout will take precedence over the global timeout.

The maximum timeout setting is 2^{32} or over 100,000 minutes, although setting the timeout to `0` on the **Global Settings** page disables the inactivity timeout (if 0 is also configured as the inactivity timeout for the user and group).

Defining and Editing Group Policies

With group access policies, all traffic is allowed by default. Additional allow and deny policies may be created by destination address or address range and by service type.

The most specific policy will take precedence over less specific policies. For example, a policy that applies to only one IP address will have priority over a policy that applies to a range of IP addresses. If there are two policies that apply to a single IP address, then a policy for a specific service (for example RDP) will take precedence over a policy that applies to all services.

Note: User policies take precedence over all group policies and group policies take precedence over all global policies, regardless of the policy definition (A ***user*** policy that allows access to all IP addresses will take precedence over a ***group*** policy that denies access to a single IP address).

To define group access policies:

1. Click **Add Policy** in the **Group Policies** section of the **Group Settings** screen. An **Add Policy** window will display.

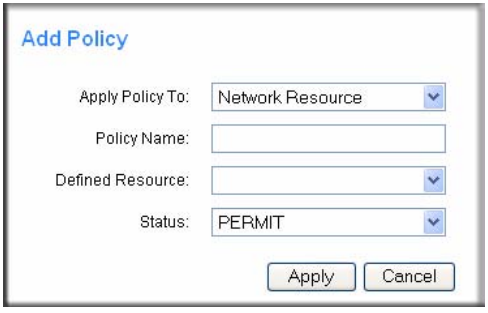

Figure 6-8

2. From the **Apply Policy To** pull-down menu, select whether the policy will be applied to a predefined network resource, an individual host, a range of addresses or all addresses.
3. Define a name for the policy in the **Policy Name** field.

Note: SSL VPN Concentrator policies apply to the destination address(es) of the SSL VPN connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the SSL VPN Concentrator through the policy engine. That type of policy would need to be defined by a firewall rule.

4. Select the appropriate policy:

- If your policy applies to a predefined network resource, select the name of the resource from the **Defined Resource** pull-down menu. For information about creating network resources, refer to Chapter 8, "Network Resources".
- If your policy applies to a specific host, enter the IP address of the local host machine in the **IP Address** field.
- If your policy applies to a network, enter the network address and subnet bit mask (0-32) in the **Network** and **Subnet Mask** fields.

5. Select the service type in the **Service** pull-down menu. If you are applying a policy to a network resource, the service type is defined in the Defined Resource field. .

Note: Network Resources are configured in **Network Resources** under the Access Administration menu on the left navigation pane.

6. Select **PERMIT** or **DENY** from the **Status** pull-down menu to either permit or deny SSL VPN connections for the specified service and host machine.
7. Click **Apply** to update the configuration. Once the configuration has been updated, the new group policy will be displayed in the table on the **Edit Group Settings** screen.

   The group policies in the **Group Policies** table are ranked by the order of priority, from the highest priority policy to the lowest priority policy.

Defining and Editing Group Bookmarks

SSL VPN Concentrator bookmarks provide a convenient way for SSL VPN users to access computers on the local area network that they will connect to frequently. Group bookmarks will apply to all members of the specific group. When group bookmarks are defined, all group members will see the defined bookmarks from the SSL VPN portal. Individual users will not be able to delete or modify group bookmarks.

To define group bookmarks:

1. Click **Add Bookmark** in the **Group Bookmarks** section of the **Group Settings** screen. An **Add Bookmark** screen will display.

   When group bookmarks are defined, all group members will see the defined bookmarks from the SSL VPN Portal. Individual group members will not be able to delete or modify group bookmarks.

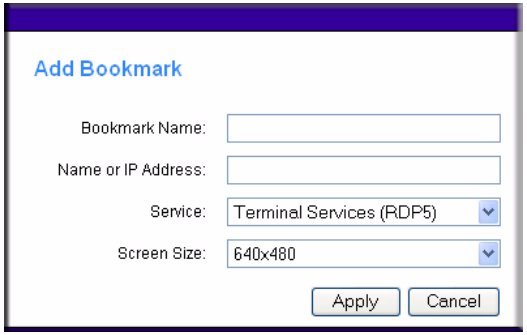

Figure 6-9

2. Enter a descriptive name in the **Bookmark Name** field.
3. Enter the domain name or the IP address of a host machine on the LAN in the **Name or IP Address** field.
4. Select the service type from the drop-down **Service** menu.
5. If Terminal Services (RDP5) is selected, select the screen size that the bookmark will use from the **Screen Size** drop-down menu.)
6. Click **Apply** to update the configuration. Once the configuration has been updated, the new group bookmark will be displayed on the **Group Settings** window. in the Group Bookmarks table.

Deleting a Group

To delete a group:

1. Click the name of the group that you wish to remove from the Groups table. The **Group Settings** window will display.
2. In the **Group Settings** window, click **Delete Group**. The **Users and Groups** window will display and the deleted group will no longer appear in the list of defined groups.

> **Note:** A group cannot be deleted if ***users*** have been added to the group or if the group is the default group created for an authentication domain.

You can also delete a group by clicking its **Delete** link.

To delete a group that is the default group for an authentication domain:

1. Delete the corresponding domain (you cannot delete the group in the **Group Settings** window).
2. If the group is not the default group for an authentication domain, first delete all users in the group. Then you should be able to delete the group on the **Group Settings** page.

	Note: The default group “geardomain” cannot be deleted.

Users Configuration

SSL VPN Concentrator users are defined from the **Users and Groups** screen Select the **Users and Groups** option under the Access and Administration menu in the left navigation pane. The **Users and Groups** screen will display.

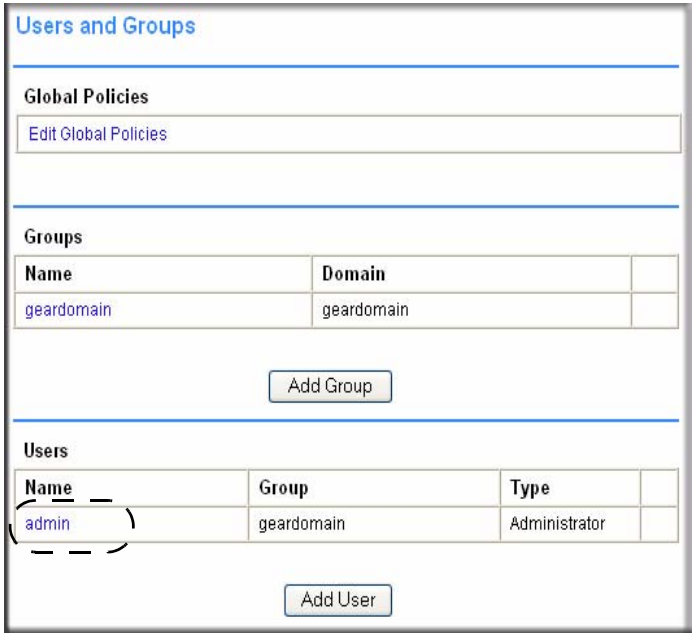

Figure 6-10

Adding a New User

To create a new user:

1. Click **Add User** on the **Users and Groups** screen. An **Add User** window will display.

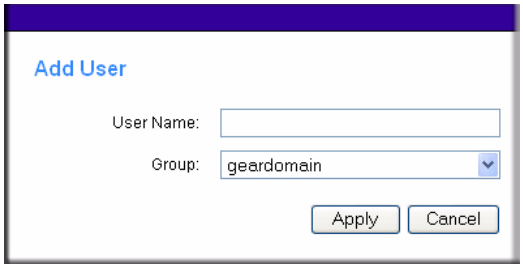

Figure 6-11

2. Enter the user name for the user in the **User Name** field. This will be the name the user will enter in order to log into the SSL VPN portal.
3. Select the name of the group to which the user belongs from the **Group** pull-down menu.
4. Click **Apply**.

   If the selected group is in a domain that uses external authentication, such as Active Directory, RADIUS, NT Domain or LDAP, then the **Add User** window will close and the new user will be added to the Users and Groups table.

	Note: Groups configured to use Radius, LDAP, NT Domain or Active Directory authentication do not require passwords because the external authentication server will validate user names and passwords.

It is only necessary to enter RADIUS, LDAP, NT and Active Directory user names if you wish to define specific policies or bookmarks per user. If users are ***not*** defined in the SSL VPN Concentrator, then **global policies** and **bookmarks** will apply to users authenticating to an external authentication server.

If the selected group is in a domain that uses internal database authentication, such as the default “geardomain” domain, then the following window will display:

Figure 6-12

5. Enter the user password in the Password field.
6. Re-enter the password in the Confirm Password field.

	Note: Both the user name and password are case-sensitive.

7. Select the user type from the User Type pull-down menu, (either User or Administrator).
8. Click **Apply** to update the configuration. Once the user has been added, the new user will be added to the table in the **Users and Groups** screen.

Editing a User

To edit a user:

1. Click the name of the user in the **Users** table on the **Users and Groups** screen. The **User Settings** window will display as shown in Figure 6-13.
   - The **Edit User Settings** section shows the **User Name**, **Group Name**, and **Domain Name**. These fields are not configurable. If information supplied in these fields need to be modified, then remove the user by clicking **Delete User** and then recreate the user with the correct information.
   - If the user authenticates to an external authentication server, then the **User Type** and **Password** fields will not be shown. The password fields are not configurable because the authentication server will validate the password. The user type is not configurable because the SSL VPN Concentrator only allows users that authenticate to the internal user database to have administrative privileges.

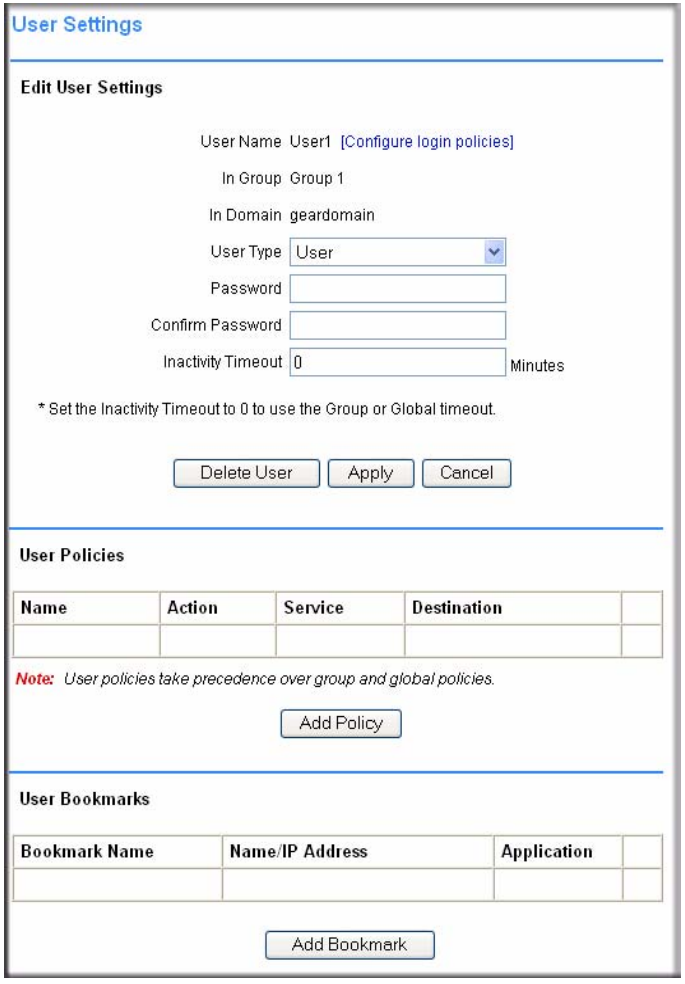

Figure 6-13

2. Enter the new user password in the **Password** field to modify the user password.
3. Enter the password again in the **Confirm Password** field.
4. Click **Apply** to update the configuration

To change the user inactivity timeout:

1. Enter the number of minutes of inactivity to allow in the **Inactivity Timeout** field.
2. Click **Apply** to save the configuration changes.

Defining and Editing User Policies

To define user access policies:

1. Click **Add Policy** on the **Edit User Settings** screen. An **Add Policy** window will display.

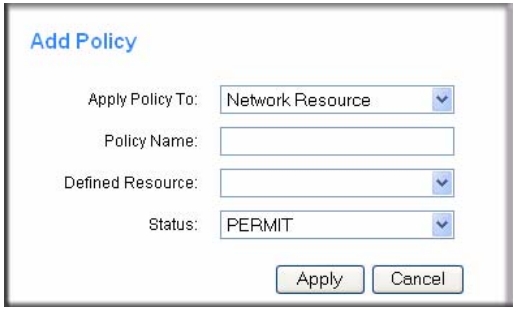

Figure 6-14

2. In the **Apply Policy To** pull-down menu, select whether the policy will be applied to a predefined network resource, an individual host, a network or all addresses.
3. Enter a name for the policy in the **Policy Name** field.

	SSL VPN Concentrator policies apply to the destination address(es) of the SSL VPN connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the SSL VPN Concentrator through the policy engine.

   - If your policy applies to a predefined network resource, select the name of the resource from the **Defined Resource** menu. For information about creating network resources, refer to Chapter 8, “Network Resources”.
   - If your policy applies to a specific host, enter the IP address of the local host machine in the **IP Address** field.
   - If your policy applies to a network, enter the network address in the **Network Address** field and the subnet mask in the **Subnet Mask** field.
4. Select the service type from the **Service** pull-down menu. If you are applying a policy to a network resource, the service type is defined in the network resource.
5. Select **PERMIT** or **DENY** from the **Status** pull-down menu to either permit or deny SSL VPN connections for the specified service and host machine.

6. Click **Apply** to update the configuration. Once the configuration has been updated, the new policy will be displayed in the **Edit User Settings** window.

   The user policies will be displayed in the **Edit Users Settings** screen in the **User Policies** table in the order of priority, from the highest priority policy to the lowest priority policy.

Defining and Editing a User Bookmarks

To define user bookmarks:

1. Click **Add Bookmark** on the **Edit User Settings** screen. An **Add Bookmark** window will display.

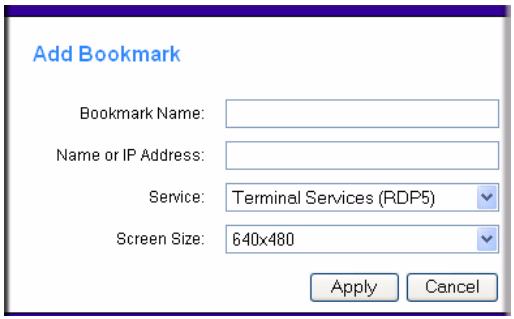

Figure 6-15

   When user bookmarks are defined, the user will see the defined bookmarks from the SSL VPN portal. Individual user members will not be able to delete or modify bookmarks created by the administrator.

2. Enter a descriptive name in the **Bookmark Name** field.
3. Enter the domain name or the IP address of a host machine on the LAN in the **Name or IP Address** field.
4. Select the service type in the **Service** pull-down menu.
5. Select the screen size the bookmark will use to display data from the **Screen Size** pull-down menu.
6. Click **Apply** to update the configuration. Once the configuration has been updated, the new user bookmark will be displayed in the **User Bookmarks** table on the **Edit User Settings** screen.

Deleting a User

To delete a user:

1. Click the **Delete** link adjacent to the users name in the **Users** table. The user will be removed from the table in the **Users and Groups** window, or
2. Click the user name that you wish to remove. The **Edit User Settings** window will display.
3. In the **Edit User Settings** window, click **Delete User.** Once deleted, the user will be removed from the table in the **Users and Groups** window.

	**Note:** A user cannot be deleted if the user is the only user defined with administrative privileges

Active Directory Authentication Servers for Group Policies and Bookmarks

Active Directory authentication servers support a group and user structure that can be queried when an Active Directory user logs in. This means that you can create policies and bookmarks for Active Directory users at the group level, without needing to define Active Directory users in the SSL VPN Concentrator. When a user logs in, if no corresponding user name is configured in the SSL VPN Concentrator, then it will query the Active Directory server for the list of groups that the user belongs to. If any of the same groups are defined in the SSL VPN Concentrator, then policies and bookmarks for the first Windows Active Directory group that matches a group configured in the SSL VPN Concentrator will be applied to the user.

Once you create an Active Directory domain, you can add groups that correspond with groups on your Active Directory server. If the Active Directory user is configured in the SSL VPN Concentrator, then the SSL VPN Concentrator will ignore the group information provided by the Active Directory and, instead, implement policies and bookmarks based on the user settings and the settings of the group to which the user belongs.

	**Note:** Because other authentication services do not have the same hierarchal structure and group definitions as Active Directory, if you want to apply specific policies or bookmarks to a group of RADIUS, NT, or LDAP users, you must add each user on the **Users and Groups** screen.

LDAP Authentication Domains for Group Policies and Bookmarks

LDAP (Lightweight Directory Access Protocol) is a standard for querying and updating a directory. Since LDAP supports a multilevel hierarchy (for example, groups or organizational units), the SSL VPN Concentrator can query this information and provide specific group policies or bookmarks based on LDAP attributes. By configuring LDAP attributes, the SSL VPN Concentrator administrator can leverage the groups that have already been configured in an LDAP or Active Directory database, rather than manually recreating the same groups in the SSL VPN Concentrator.

Once an LDAP authentication domain is created, a default LDAP group will be created with the same name as the LDAP domain name. Although additional groups may be added or deleted from this domain, the default LDAP group may not be deleted.

For an LDAP group, you may define LDAP attributes. For example, you can specify that users in an LDAP group must be members of a certain group or organizational unit defined on the LDAP server. Or you can specify a unique LDAP distinguished name.

Note: The Microsoft Active Directory database uses an LDAP organization schema. The Active Directory database may be queried using Kerberos authentication (the standard authentication type; this is labeled “Active Directory” domain authentication in the SSL VPN Concentrator), NTLM authentication (labeled “NT Domain” authentication in the SSL VPN Concentrator), or using LDAP database queries. So, an LDAP domain configured in the SSL VPN Concentrator can authenticate to an Active Directory server.

To add an LDAP authentication domain, see “Authentication Domains” in Chapter 7.

Sample LDAP Attributes

You may enter up to 4 LDAP attributes per group. The following are some example LDAP attributes of Active Directory LDAP users:

```
name=”Administrator”
memberOf=”CN=Terminal Server Computers,CN=Users,DC=netgearnetworks,
DC=net”objectClass=”user”
msNPAllowDialin=”FALSE”
```

LDAP Attribute Rules

- If multiple attributes are defined for a group, ***ALL*** attributes must be met by LDAP users.
- If no attributes are defined, then any user authorized by the LDAP server can be a member of the group.
- If multiple groups are defined and a user meets all the LDAP attributes for two groups, then the user will be considered part of the group with the most LDAP attributes defined. If the matching LDAP groups have an equal number of attributes, then the user will be considered a member of the group based on the alphabetical order of the groups.
- If an LDAP user fails to meet the LDAP attributes for all LDAP groups configured on the SSL VPN Concentrator, then the user will not be able to log into the portal. So the LDAP attributes feature not only allows the administrator to create individual rules based on the LDAP group or organization, it also allows the administrator to only allow certain LDAP users to log into the portal.

Sample LDAP Users and Attributes Settings

If a user is manually added to a LDAP group, then the user setting will take precedence over LDAP attributes.

For example:

- An LDAP attribute `objectClass="Person"` is defined for group **Group1** and an LDAP attribute `memberOf="CN=WINS Users,DC=netgearnetworks,DC=net"` is defined for **Group2**.
- If user **Jane** is defined by an LDAP server as a member of the **Person** object class, but is NOT a member of the **WINS Users** group, **Jane** will be a member of the SSL VPN Concentrator **Group1**.
- But if the administrator manually adds the user **Jane** to the SSL VPN Concentrator **Group2**, then the LDAP attributes will be ignored and **Jane** will be a member of **Group2**.

Querying an LDAP Server

If you would like to query your LDAP or Active Directory server to find out the LDAP attributes of your users, there are several different methods. From a machine with LDAPsearch tools (for example a Linux machine with OpenLDAP installed) run the following command:

```
ldapsearch -h 10.0.0.5 -x -D "cn=demo,cn=users,dc=netgearnetworks,dc=net"
-w demo123 -b "dc=netgearnetworks,dc=net" > /tmp/file
```

Where:

- `10.0.0.5` is the IP address of the LDAP or Active Directory server
- `"cn=demo,cn=users,dc=netgearnetworks,dc=net"` is the distinguished name of an LDAP user
- `demo123` is the password for the user `demo`
- `"dc=netgearworks,dc=net"` is the base domain that you are querying
- `> /tmp/file` is optional and defines the file where the LDAP query results will be saved.

For further information on querying an LDAP server from a Window server, please see: *http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/8196d68e-776a-4bbc-99a6-d8c19f36ded4.mspx*

NT and RADIUS Domain Servers for Group Policies and Bookmarks

For authentication to RADIUS or Microsoft NT domains (using Kerberos), you can individually define AAA users and groups. This is not required, but it allows you to create separate policies or bookmarks for individual AAA users.

When a user logs in, the SSL VPN Concentrator will validate with the appropriate RADIUS or NT server that the user is authorized to log in. If the user is authorized, the SSL VPN Concentrator will check to see if a user exists in the SSL VPN Concentrator **Users and Groups** database. If the user is defined, then the policies and bookmarks defined for the user will apply.

For example, if you create a RADIUS domain in the SSL VPN Concentrator called “Miami RADIUS server”, you can add users to groups that are members of the “Miami RADIUS server” domain. These user names must match the names configured in the RADIUS server. Then, when users log in to the portal, policies, bookmarks and other user settings will apply to the users. If the AAA user does not exist in the SSL VPN Concentrator, then only the global settings, policies and bookmarks will apply to the user.

For adding new RADIUS or Microsoft NT domain servers, see “Authentication Domains” in Chapter 7.

Chapter 7
Domains and Layouts

This chapter explains how to define authentication domains, such as RADIUS, NT Domain, LDAP, and Active Directory configuration.

It describes:

Authentication Domains

To view the SSL VPN Concentrator **Domains** window from the Administrative User Interface, click the **Domains** option under the Access Administration menu in the left navigation pane.

Figure 7-1

In order to create access policies, you must first create authentication domains. By default, the **geardomain** authentication domain is already defined. The SSL VPN Concentrator domain is the SSL VPN Concentrator internal user database.

Additional domains may be created that require authentication to remote authentication servers. The SSL VPN Concentrator supports RADIUS (PAP, CHAP, MSCHAP, and MSCHAPV2), LDAP, NT Domain, and Active Directory authentication in addition to internal user database authentication.

All of the configured domains will be listed in the table in the **Domains** window. The domains are listed in the order in which they were created.

Local User Database Authentication

You may create multiple domains that authenticate users with users and passwords stored on the SSL VPN Concentrator. This is necessary if you wish to display different portal layouts (such as SSL VPN portal pages, themes, etc.) to different users.

To add a new authentication domain:

1. Click **Add Domain**. An **Add Domain** window similar to the following will display.

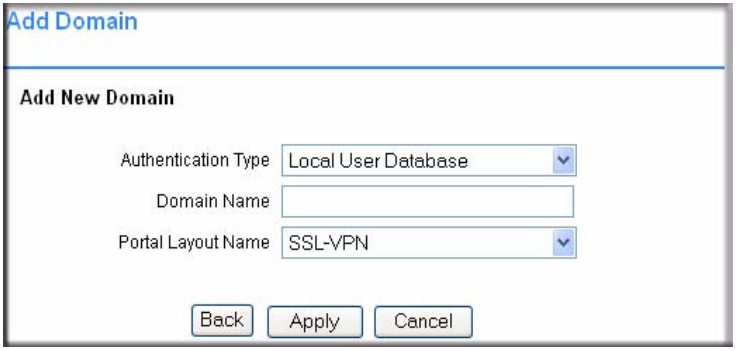

Figure 7-2

2. Select **Local User Database** from the **Authentication Type** pull-down menu.
3. Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SSL VPN portal.
4. Select the name of the layout in the **Portal Layout Name** pull-down menu. The default layout is **SSL-VPN**. Additional layouts may be defined in the **Portal Layouts** screen.
5. Check the **Require client digital certificates** radio box to force users to supply a valid digital certificate before granting access. The CNAME of the client certificate must match the user name that the user supplies to log in and the certificate must be generated by a certificate authority (CA) that is trusted by SSL VPN Concentrator.

6. Click **Apply** to update the configuration. Once the domain has been added, the domain will be added to the table on the **Domains** screen

RADIUS Authentication

To create a domain with Radius authentication:

1. Click **Add Domain**. An **Add Domain** window will be displayed.
2. Select a **RADIUS** domain from the **Authentication Type** pull-down menu. The Add Domain window displays the fields for a domain for Radius authentication.

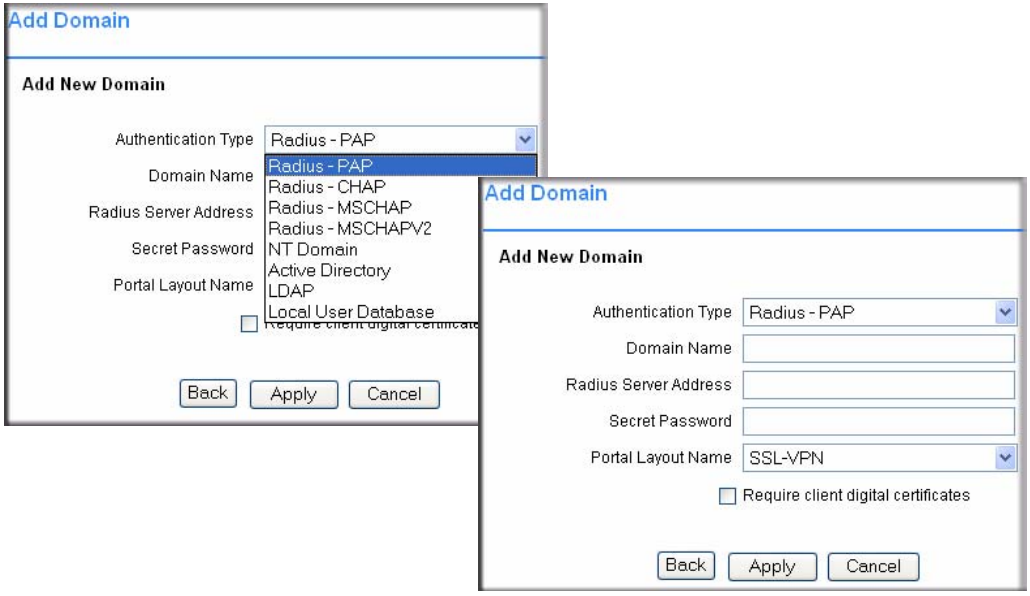

Figure 7-3

3. Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SSL VPN portal.
4. Enter the IP address or domain name of the Radius server in the **Radius Server Address** field.
5. If required by the Radius server, enter an authentication secret in the **Secret Password** field.
6. Select the name of the layout from the **Portal Layout Name** drop-down menu. The default layout is **SSL-VPN**. Additional layouts may be defined in the **Portal Layouts** page.

7. Check the **Require client digital certificates** checkbox to force users to supply a valid digital certificate before granting access. The CNAME of the client certificate must match the user name that the user supplies to log in and the certificate must be generated by a certificate authority (CA) that is trusted by SSL VPN Concentrator.
8. Click **Apply** to update the configuration. Once the domain has been added, the domain will be added to the table on the **Domains** screen.

NT Domain Authentication

To configure NT Domain authentication, click **Add Domain**. An **Add Domain** window will be displayed. In the **Add Domain** window.

1. Select **NT Domain** from the **Authentication Type** menu. The NT Domain configuration fields will be displayed. The Add Domain window displays the fields for a domain with NT authentication:

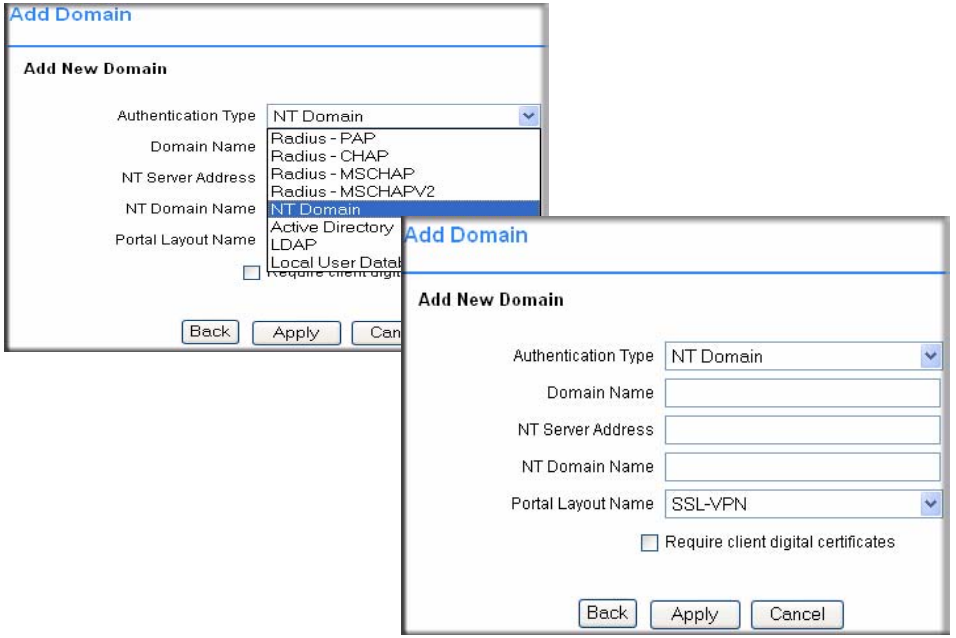

Figure 7-4

2. Enter a descriptive name for the authentication domain in the SSL VPN Concentrator **Domain Name** field. This is the domain name selected by users when they authenticate to the SSL VPN portal. It may be the same value as the **NT Domain Name**.

3. Enter the IP address or host and domain name of the server in the **NT Server Address** field.
4. Enter the NT authentication domain in the **NT Domain Name** field. This is the domain name configured on the Windows authentication server for network authentication.
5. Select the name of the layout from the **Portal Layout Name** pull-down menu The default layout is **SSL-VPN**. Additional layouts may be defined in the **Portal Layouts** page.
6. Check the **Require client digital certificates** checkbox to force users to supply a valid digital certificate before granting access. The CNAME of the client certificate must match the user name that the user supplies to log in and the certificate must be generated by a certificate authority (CA) that is trusted by the SSL VPN Concentrator.
7. Click **Apply** to update the configuration. Once the domain has been added, the domain will be added to the table in the **Domains** screen.

LDAP Authentication

To configure LDAP authentication, click **Add Domain**. An **Add Domain** window will be displayed. In the **Add Domain** window:

1. Select **LDAP** from the **Authentication Type** menu. The LDAP domain configuration fields will be displayed.The Add Domain Window displays the fields for a domain with LDAP authentication

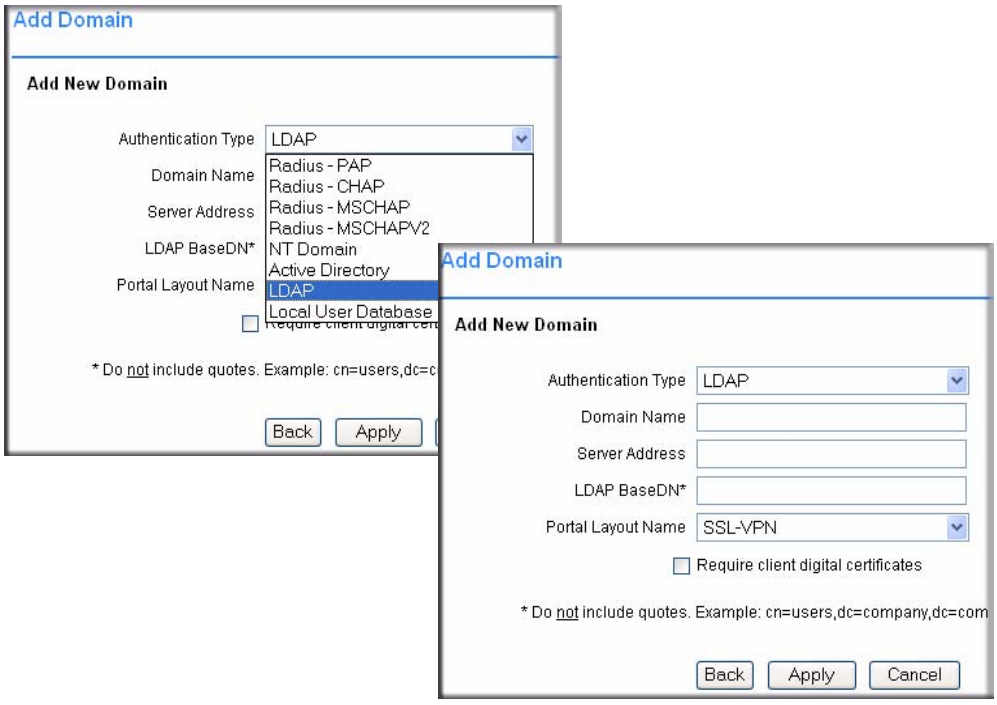

Figure 7-5

2. Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SSL VPN portal. It can be the same value as the **Server Address** field.
3. Enter the IP address or domain name of the server in the **Server Address** field.
4. Enter the search base for LDAP queries in the **LDAP BaseDN** field. An example of a search base string is

```
CN=Users,DC=yourdomain,DC=com
```

	Note: Do not include quotes (“ ”) in the LDAP BaseDN field.

5. Select the name of the layout from the **Portal Layout Name** drop-down menu. The default layout is **SSL-VPN**. Additional layouts may be defined in the **Portal Layouts** page.

6. Check the **Require client digital certificates** checkbox to force users to supply a valid digital certificate before granting access. The CNAME of the client certificate must match the user name that the user supplies to log in and the certificate must be generated by a certificate authority (CA) that is trusted by SSL VPN Concentrator.
7. Click **Apply** to update the configuration. Once the domain has been added, the domain will be added to the table on the **Domains** screen.

Active Directory Authentication

To configure Windows Active Directory authentication:

1. Click **Add Domain**. An **Add Domain** window will display.

Note: Of all types of authentication, Active Directory authentication is the most error prone. If you are unable to authenticate using Active Directory, please read the troubleshooting procedure at the end of this section.

2. Select **Active Directory** from the **Authentication Type** menu. Fields for Active Directory configuration will display.

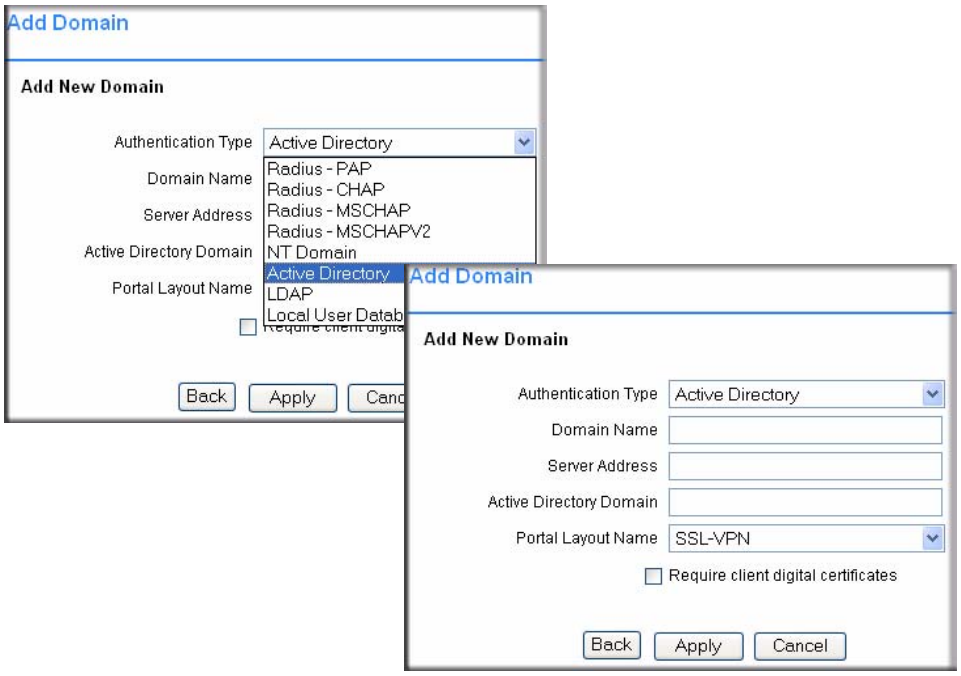

Figure 7-6

3. Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SSL VPN portal. It can be the same value as the **Server Address** field or the **Active Directory Domain** field depending on your network configuration.
4. Enter the IP address or host and domain name of the Active Directory server in the **Server Address** field.
5. Enter the Active Directory domain name in the **Active Directory Domain** field.
6. Select the name of the layout from the **Portal Layout Name** menu The default layout is **SSL-VPN**. Additional layouts may be defined in the **Portal Layouts** page.
7. Check the **Require client digital certificates** checkbox to force users to supply a valid digital certificate before granting access. The CNAME of the client certificate must match the user name that the user supplies to log in and the certificate must be generated by a certificate authority (CA) that is trusted by the SSL VPN Concentrator.
8. Click **Apply** to update the configuration. Once the domain has been added, the domain will be added to the table on the **Domains** screen

If your users are unable to connect via Active Directory, verify the following:

1. The time settings between the Active Directory server and the SSL VPN Concentrator must be synchronized. Kerberos authentication, used by Active Directory to authenticate clients, permits a maximum of a 15-minute time difference between the Windows server and the client (the SSL VPN Concentrator). The easiest way to solve this issue is to configure Network Time Protocol on the **Date and Time** screen and check that the server's time settings are also correct.
2. Confirm that your Windows server is configured for Active Directory authentication. If you are using a Window NT 4.0 server, then your server only supports NT Domain authentication. Typically, Windows 2000 and 2003 servers are also configured for NT Domain authentication to support legacy Windows clients.

Deleting a Domain

To delete a domain, click the **Delete** link in the **Domains** table for the domain you wish to remove. Once the SSL VPN Concentrator has been updated, the deleted domain will no longer be displayed in the table in the **Domains** table.

	**Note:** The SSL VPN Concentrator **"geardomain"** domain cannot be deleted.

SSL VPN Concentrator Portal Layouts

The SSL VPN **Portal Layouts** screen allows you to create a custom page that mobile users will see when they log into the portal. Because the page is completely customizable, it provides the ideal way to communicate remote access instructions, support information, technical contact info or VPN-related news updates to remote users. The page is also well-suited as a starting page for restricted users; if mobile users or business partners are only permitted to access a few files or web URLs, the page you create will only show those links relevant to these users.

To view the **Portal Layout** screen, click **Portal Layouts** under the SSL VPN Portal menu on the left navigation pane. A window similar to the following will display.

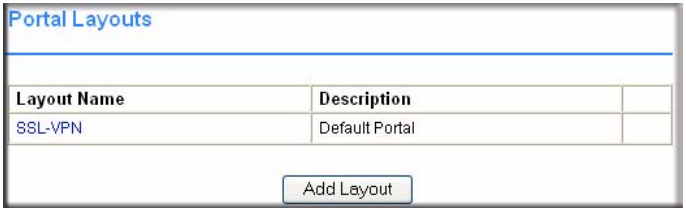

Figure 7-7

Adding Portal Layouts

The SSL VPN Concentrator administrator may define individual layouts for the SSL VPN portal. The layout configuration includes the theme, menu layout, portal pages to display, portal application icons to display, and web cache control options.

A default portal layout is the **SSL-VPN** portal. Additional portal layouts can be added and modified.

Note: To apply a portal layout to a domain, add a new domain and select the portal layout from the **Portal Layout Name** menu on the domain configuration page. The selected portal layout will be applied to all users in the new domain.

To add a new portal layout:

1. Click **Portal Layouts** under the **SSL VPN Portal** menu on the left navigation pane and click **Add Layout.** The **Portal Layout** page will display.
2. In the **Portal Layout and Theme Name** section:
   a. Enter a descriptive name for the portal layout in the **Portal Layout Name** field. This name will be part of the path of the SSL VPN portal URL.

      For example, if your SSL VPN portal is hosted at https://vpn.company.com, and you created a portal layout named “sales”, then users will be able to access the sub-site at https://vpn.company.com/portal/sales.

      Only alphanumeric characters, hyphen (-), and underscore (_) are accepted for the **Portal Layout Name**. If other types of characters or spaces are entered, the layout name will be truncated before the first non-alphanumeric character. Please note that unlike most other URLs, this name is case sensitive.

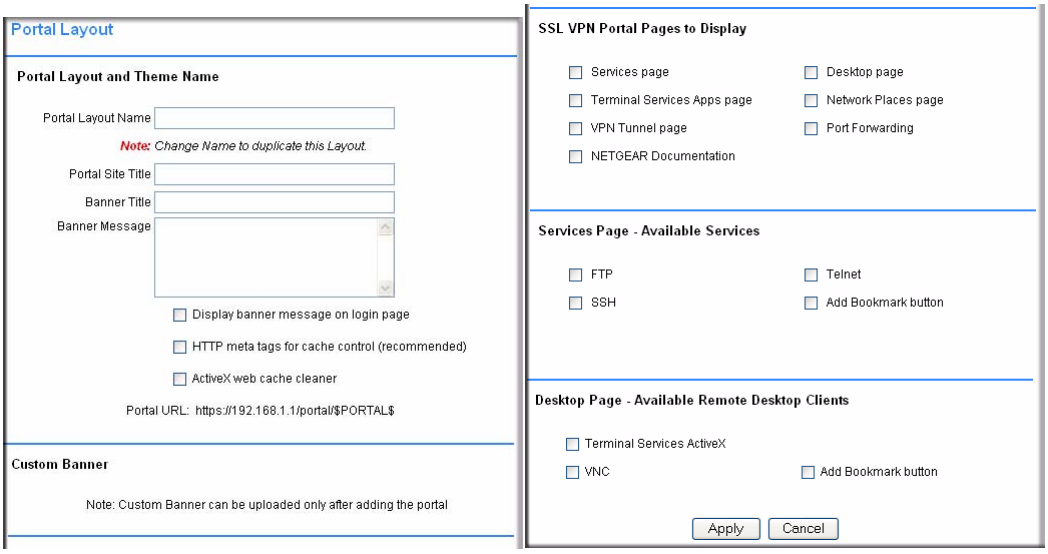

Figure 7-8

b. Enter the title for the web browser window in the **Portal Site Title** field.

c. If you wish to display a banner message to users before they log in to the portal, enter the banner title text in the **Banner Title** field. Also enter the banner message text in the **Banner Message** text area. Then check the **Display banner message on login page** radio button to show the banner title and banner message text on the Login screen.

d. Check the **Enable HTTP meta tags for cache control** radio box to apply HTTP meta tag cache control directives to this Portal Layout. Cache control directives include:

```
<meta http-equiv=”pragma” content=”no-cache”>

<meta http-equiv=”cache-control” content=”no-cache”>

<meta http-equiv=”cache-control” content=”must-revalidate”>
```

These directives help prevent clients browsers from caching SSL VPN portal pages and other web content.

	Note: Enabling HTTP meta tags is strongly recommended for security reasons and to prevent out-of-date web pages, themes and data being stored in users' web browser cache

e. Check the **ActiveX web cache cleaner** radio box to load an ActiveX cache control when users log in to the SSL VPN portal.

The web cache cleaner will prompt the user to delete all temporary Internet files, cookies and browser history when the user logs out or closes the web browser window. The ActiveX web cache control will be ignored by web browsers that don't support ActiveX.

3. Select the portal pages you wish users to access in the **SSL VPN Portal Pages to Display** section. Any pages that are not selected will not be visible from the portal navigation menu.

Note: If you hide portal pages or applications, you should also ***create SSL VPN access policies that deny access*** to the corresponding applications. The portal layout only affects the look and feel of the portal, but it does not prevent users from accessing hidden sites.

4. Select the services that users should be able to access in **Services Page – Available Services**. Only the corresponding service icons will be visible on the **Services** page.

5. Select the desktop clients that users should be able to access in **Desktop Page – Available Remote Desktop Clients**. Only the corresponding service icons will be visible on the **My Desktop** page.

6. Click **Apply** to confirm your settings.

Note: An administrator can customize the portal layout by uploading a gif file for the banner image. However, the custom banner can be uploaded only after adding the portal.

Now you can apply the portal layout to one or more authentication domains.

If you selected the option **Terminal Services Apps page** (in the **SSL VPN Portal Pages to Display** section), then the **Portal Layout** screen will expand to include an **Applications Page - Available Terminal Services Applications** section. You can now add Terminal Services application icons to display in the Applications page.

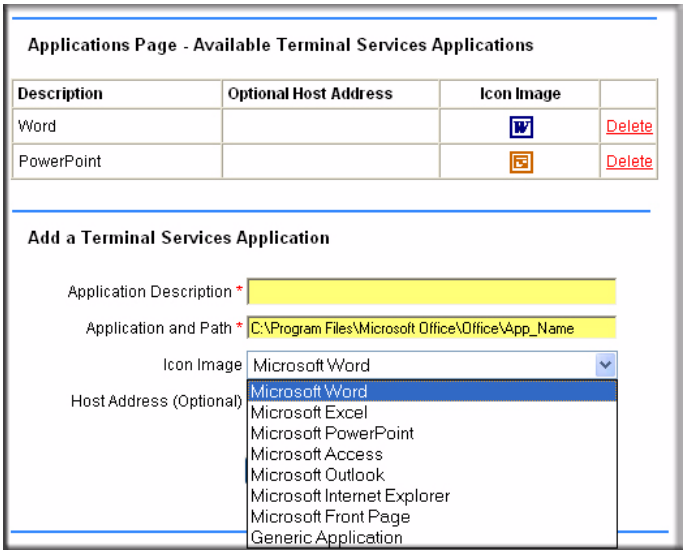

Figure 7-9

To add a Terminal Services Application:

1. Enter a description of the application in the **Application Description** field. This name will be shown beneath the application icon on the SSL VPN Portal Applications page.
2. Enter the path and application name of the Terminal Services application in the **Application and Path** field.

> **Note:** To launch a Terminal Services application individually, the Terminal Server must be run in Application mode. In addition, the application must be installed through the **Control Panel Add/Remove Programs**. For more information, see the NETGEAR Support Site.

3. Select an image to show on the Applications page from the **Icon Image** menu.
4. Click **Add Application** to add the new application to the SSL VPN Portal **Applications** page.

Apply the portal layout to one or more SSL VPN Concentrator authentication domains.

Customizing the Banner

An administrator can further customize the portal by uploading a a customized image for the banner.

To upload a banner image:

1. On the **Portal Layout** screen (see Figure 7-8 on page 7-11), click **Upload Banner**. The **Custom Banner** screen will display.

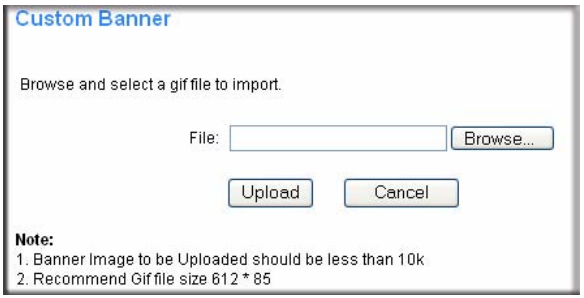

Figure 7-10

2. Click **Browse** to locate and upload a .gif file. If upload is successful, two new buttons will appear—**View Banner** and **Delete Banner** on the **Portal Layout** screen.

   Click **View Banner** to view the uploaded banner. Click **Delete Banner** to delete an uploaded banner.

Duplicating and Editing Portal Layouts

You can edit the features of an existing portal; for example, create a banner or banner message that displays at the top of the page; or show or hide all applicable bookmarks (user, group, and global) for each user. You can, optionally, upload an HTML file. You can also create another portal with all of the features of the existing portal by changing the existing portal layout name.

	Note: Changing the portal name will only duplicate the portal and will not rename the existing portal

To add a new Portal by editing an existing Portal layout:

1. Click **Portal Layouts** under the **SSL VPN Portal** menu on the left navigation pane. The **Portal Layouts** screen will display.
2. In the Portal Layouts table, click the Portal Layout name you wish to duplicate. The **Portal Layout** screen of the selected Portal will display.
3. Enter the new name in the **Portal Layout Name** field. The new title will be displayed at the top of the page.

4. Click **Apply.** A new portal will be created with the same features as the existing portal and will be displayed in the **Portal Layouts table.**

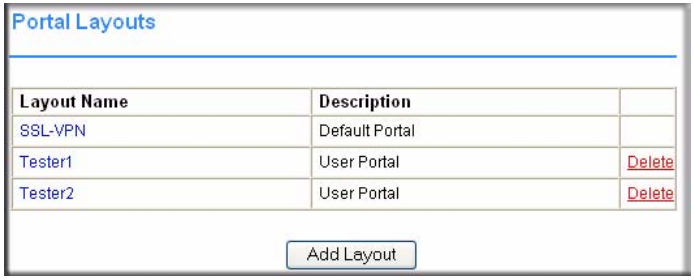

Figure 7-11

To modify the features of an existing portal:

1. Click **Portal Layouts** under the **SSL VPN Portal** menu on the left navigation pane. The **Portal Layouts** screen will display.
2. In the **Layout Name** column, click the portal you want to edit. The **Portal Layouts** screen will display.
3. Enter a new **Banner Title** and **Banner message**, and check the **Display banner message on login page** radio box to display a custom message at the top of the new page.
4. Modify any of the services in the **SSL VPN Portal Pages to Display, Services Page – Available Services**, or **Desktop Page – Available Remote Desktop Clients** sections of the **Portal Layouts** screen. For example:
   - Leave the **Desktop Page/Add Bookmark button** radio box checked to display all applicable user, group and global bookmarks in a single table on the desktop page.
   - Leave the **Display banner message on login page** radio box checked, and enter a custom message to be displayed at the top of the portal login page in the **Banner message** field. Enter a plain text message or include HTML and JavaScript tags. The maximum length of the login page message is 4096 characters.
5. Click **Apply** to update the home page content.

Note: The **Available Terminal Services Applications** displayed in the edited Portal Layout page will apply to the new page if the Application and Path are the same. If the path is not the same, when the new page is created the Applications Services will no longer be available.

Advanced Portal Page Layout Specifications

For most SSL VPN administrators, a plain text page message and a list of links to network resources will provide the prefect portal desktop page. But for the more advanced administrator that want to display additional content, please note:

- The portal page is displayed in an IFRAME--internal HTML frame.
- The width of the iframe is 542 pixels, but since there is a 29 pixel buffer between the navigation menu and the content, the available workspace is **513 pixels**.
- You can upload a custom HTML file which will be displayed below all other content on the home page. You can also add HTML tags and JavaScript to the **Banner Message**.
- Since the uploaded HTML file will be displayed after other content, do not include <head> or <body> tags in the file.

Chapter 8
Network Resources

This chapter explains how to define network resource groups. Network resources facilitate creating and updating access policies.

Network Resources are groups of host names, IP addresses and IP address ranges. By defining resource objects, you can more quickly configure network policies. This is because you will not need to redefine the same set of IP addresses or address ranges when configuring the same access policies for multiple users.

Defining Network Resources is optional; smaller organizations can choose to create access policies using individual IP addresses or IP networks rather than predefined Network Resources. But for most organizations, it is recommended that you use Network Resources. If your server or network configuration changes, by using Network Resources you can perform an update quickly instead of individually updating all of the user and group policies.

To configure a network policy:

1. Select **Network Resources** under the **Access Administration** menu on the left navigation pane. The **Network Resources** screen will display.

Figure 8-1

2. Click **Add Resource**. An **Add Network Resource** screen similar to the following will display.

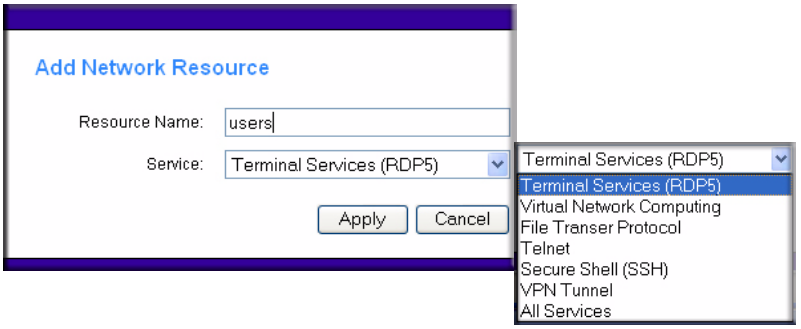

Figure 8-2

3. In the **Resource Name** field, enter a name for the Network Resource.
4. From the **Services** pull-down menu, select the type of service to which the Network Resource will apply.
5. Click **Apply**. The new Network Resource will display in the table on the **Network Resources** screen.

Figure 8-3

To edit the Network Resource.

1. Click the name of the resource in the **Resource Name** column in the table on the **Network Resources** screen. The **Edit Network Resource** screen will display.

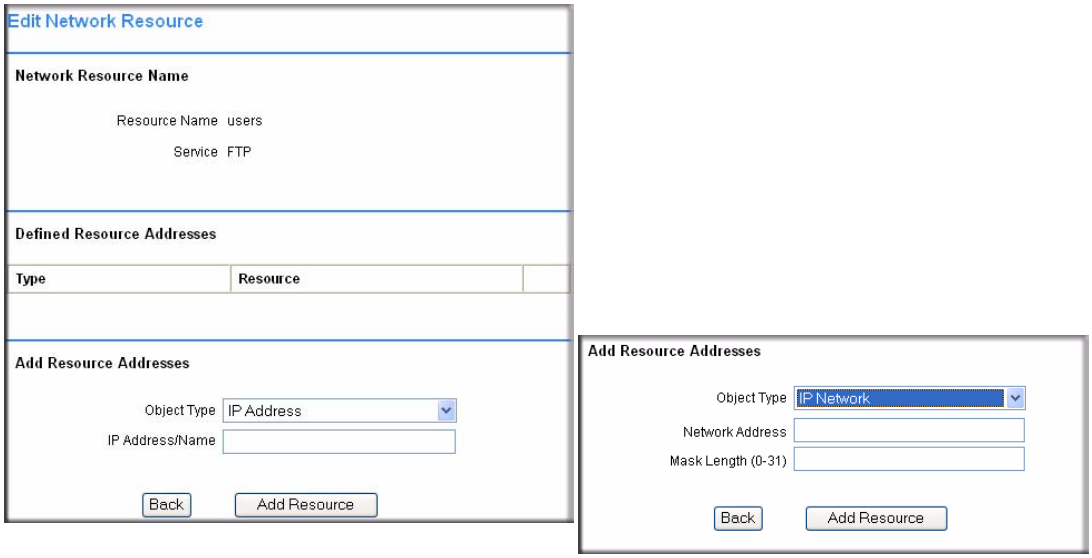

Figure 8-4

2. From the **Object Type** pull-down menu under **Add Resource Addresses**, select either **IP Address** or **IP Network**:

   - If **IP Address** was selected, enter an IP address or fully qualified domain name in the **IP Address/Name** field.
   - If **IP Network** was selected, enter the IP network address in the **Network Address** field. Enter the mask length in the **Mask Length (0-31)** field.

3. Click **Add Resource** to add the IP address or IP network to the Network Resource. The new configuration will be displayed in the **Defined Resource Addresses** table, as shown in the example below.

   You may define up to 128 addresses or address ranges per Network Resource.

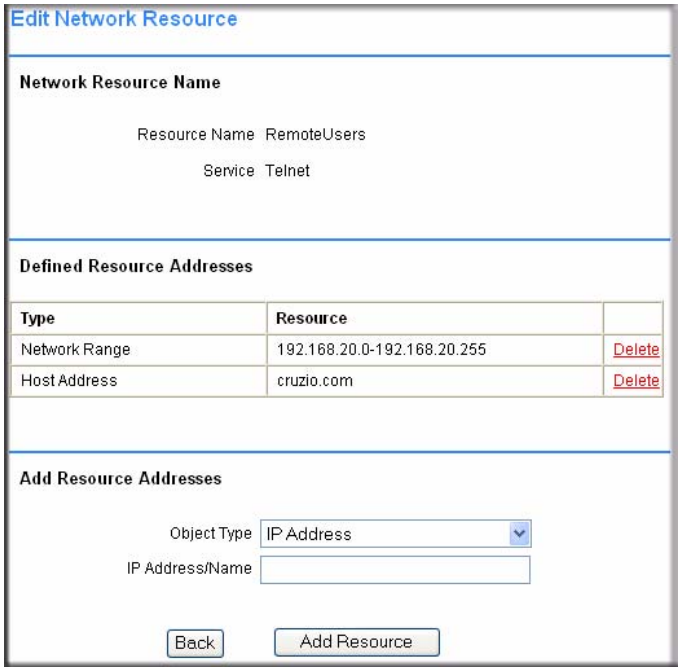

Figure 8-5

To delete a defined resource, click **Delete** in the **Defined Resource Addresses** table adjacent to the resource you wish to delete.

To create policies based on network objects, see Chapter 6, “Group and User Access Policies”, for instructions on configuring Access Policies.

Chapter 9
VPN Tunnel Client

This chapter describes the configuration for a VPN Tunnel Client, an SSL VPN client that is deployed from the SSL VPN portal. It covers:

- Adding IP Address Ranges
- Adding Routes for VPN Tunnel Clients

Beyond what is defined in "Logging in to the Management Interface" on page 2-4, the VPN Tunnel Client has some specific operating requirements. For

- **Mac OS**. VPN Tunnel supports Version 1.4 (Tiger).
- **Browsers.** The Firefox browser is not supported.

The number of VPN Tunnel Client sessions your installation of SSL VPN Concentrator will support concurrently is dependent on the hardware configuration of your SSL VPN Concentrator server.

SSL VPN Client Configuration

There are several different scenarios you can use to set up SSL VPN client addresses and routes. The following is a simple network setup. For more complex network configurations, see the SSL VPN network scenarios document referenced in Appendix B, "Related Documents".

The VPN Tunnel Client provides a PPP (point-to-point) connection between the client and the SSL VPN Concentrator. When remote users connect using VPN over SSL, a virtual network interface is created with IP settings dynamically assigned by the SSL VPN Concentrator. In addition, DNS and WINS server settings are also assigned by the SSL VPN Concentrator. DNS and WINS settings allow the VPN Tunnel Client to contact machines on the corporate network by host name or domain name. The DNS and WINS settings assigned to the VPN Tunnel Client are configured on the **Network** screen located under System Configuration on the left navigation pane.

The VPN Tunnel Client provides a point-to-point (PPP) connection and uses proxy ARP requests to locate machines on the remote network. Because the connection is a point-to-point connection, the addresses on the local network and the remote network can overlap. For example:

- The VPN Tunnel Client cannot contact a server on the corporate network if the VPN Tunnel Client's Ethernet interface shares the same IP address as the server or the SSL VPN Concentrator (i.e., if your laptop has a physical interface address of **10.0.0.45**, then you won't be able to contact a server on the remote network that also has the IP address **10.0.0.45**).
- You do not want the virtual (PPP) interface address of the VPN Tunnel Client to conflict with addresses on the corporate network. Therefore, configure an IP address range that does not directly overlap with addresses on your local network. So, if **192.168.0.1 through 192.168.0.100** are currently assigned to machines on your local network, then start the client address range at **192.168.0.101** or choose an entirely different subnet altogether.

Adding IP Address Ranges

If you choose a different subnet for the VPN Tunnel Client range than the subnet used by the corporate network, then you must:

1. Add a client route to configure the VPN Tunnel client to connect to the corporate network using the VPN tunnel.
2. Create a static route on the corporate network's firewall to forward traffic intended for the VPN Tunnel Client range to the SSL VPN Concentrator.

Once you have determined the address range you will assign to VPN Tunnel Clients, then define the address range in the SSL VPN Concentrator administrative interface.

To configure SSL VPN Tunnel client address range:

1. Click the **VPN Tunnel** option under Access Administration in the left navigation pane. The **VPN Tunnel Client** screen will display.

You may define the IP address range to assign to incoming VPN Tunnel clients in the **Client IP Address Range** section of the screen. The default range begins with 192.168.251.1 and ends with 192.168.251.254.

2. Enter the first IP address of the IP address range in the **Client Address Range Begin** field.

3. Enter the last IP address of the IP address range in the **Client Address Range End** field.

4. Click **Apply** to update the configuration.

5. Restart the SSL VPN Concentrator software if VPN Tunnel Clients are actively connected; this will force the clients to obtain a new virtual IP address.

VPN Tunnel Clients will now be able to connect to the SSL VPN Concentrator and receive a dynamic IP address in the client address range.

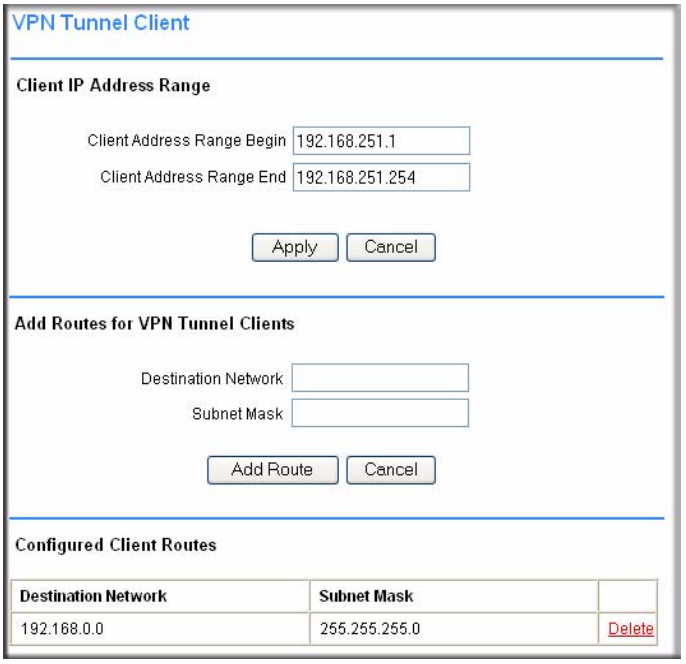

Figure 9-1

Adding Routes for VPN Tunnel Clients

The **Add Routes for VPN Tunnel Clients** section allows you to define the addresses of devices on your local network. Client routes are only required if the client address range is in a different subnet then the corporate network or if your network has multiple subnets. Client routes inform the VPN Tunnel Clients that other networks are located across the VPN over SSL tunnel by:

- The first VPN Tunnel Client assumes that addresses in the same subnet as the client IP address (PPP interface) are located across the VPN over SSL tunnel.
- The address range in the client subnet. The specific subnet is determined by the class of the IP address.
  - Addresses between 1.0.0.0 and 126.255.255.255, are **Class A** addresses; the VPN Tunnel Client will assume that all addresses with the same first octet are located across the VPN tunnel.

- Addresses between 128.0.0.0 and 191.255.255.255 are **Class B** addresses; the VPN Tunnel Client will assume that all addresses with the same first two octets are located across the VPN tunnel.
- Addresses between 192.0.0.0 and 223.255.255.255 are **Class C** addresses; the VPN Tunnel Client will assume that all addresses with the same first three octets are located across the VPN tunnel.

The subnet classes for the designated private IP address ranges are:

- **Class A subnet:** 10.0.0.0 through 10.255.255.255
- **Class B subnet:** 172.16.0.0 through 172.16.31.255.255
- **Class C subnet**: 192.168.0.1 through 192.168.255.255

If VPN Tunnel Clients need to connect to addresses on the corporate network that are not in the same subnet as the client address range, then you will need to add client routes.

To add an SSL VPN Tunnel client route:

1. In the **Destination Network** field under **Add Routes for VPN Tunnel Clients** section, enter the network address of a local area network or subnet For example, enter 192.168.0.0.
2. Enter the subnet mask of the local area network **Subnet Mask** field.
3. Click **Add Route**. The client route will be displayed in the **Configured Client Routes** table, as shown in the example in Figure 9-2.

	**Note:** You will also need to add a static route on your corporate firewall or router that directs traffic destined for the VPN Tunnel Client address range to the SSL VPN Concentrator.

4. Restart the SSL VPN Concentrator software if VPN Tunnel Clients are currently connected to the SSL VPN Concentrator. Restarting forces clients to reconnect and receive new addresses and routes.

   Now users will be able to connect to the SSL VPN Concentrator and receive a virtual IP address from the client address range.

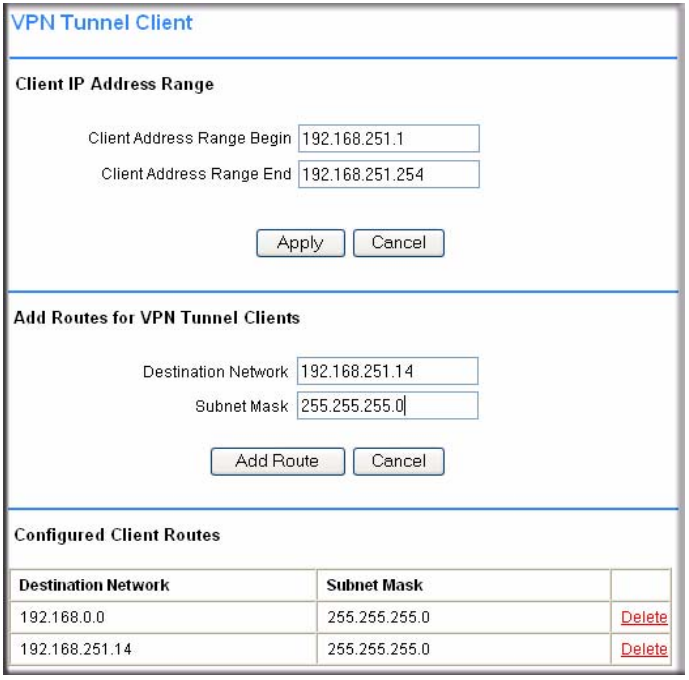

Figure 9-2

To delete a VPN Tunnel Client Route:

1. Click the **Delete** link adjacent to the client route in the **Configured Client Routes** table.
2. Restart the SSL VPN Concentrator software if VPN Tunnel Clients are currently connected to the SSL VPN Concentrator. Restarting forces clients to reconnect and receive new addresses and routes.

Chapter 10
Port Forwarding

This chapter describes the configuration for Port Forwarding, a web-based SSL VPN client that installs transparently and then creates a virtual, encrypted tunnel to the remote network. Using Port Forwarding, mobile users can access mission-critical applications such as email or mapped network drives as if they were located on the corporate network.

This chapter covers:

Port Forwarding, like VPN Tunnel, is a web-based client that installs transparently and then creates a virtual, encrypted tunnel to the remote network. However, Port Forwarding differs from VPN Tunnel in several ways. For example, Port Forwarding:

- Only supports TCP data, not UDP or other IP protocols.
- Detects and reroutes individual data streams over the Port Forwarding connection rather than opening up a full tunnel to the corporate network. So Port Forwarding is a lighter client than VPN Tunnel and installs more quickly.
- Offers more fine grained management than VPN Tunnel. Administrators define individual applications and resources that will be available to remote users. With VPN Tunnel, administrators must create access policies to block undesirable traffic at the SSL VPN Concentrator rather than at the client level.

Configuring Applications for Port Forwarding

Port Forwarding client detects and reroutes data sent by the remote users to the SSL VPN Concentrator. The **Port Forwarding** screen allows you to specify the internal addresses and applications that Port Forwarding clients may access. To configure Port Forwarding, you must define the internal host machines and TCP applications available to remote users.

To configure applications for Port Forwarding:

1. From the **Access Administration** menu in the left navigation pane, select the **Port Forwarding** option. The **Port Forwarding** configuration screen will display.

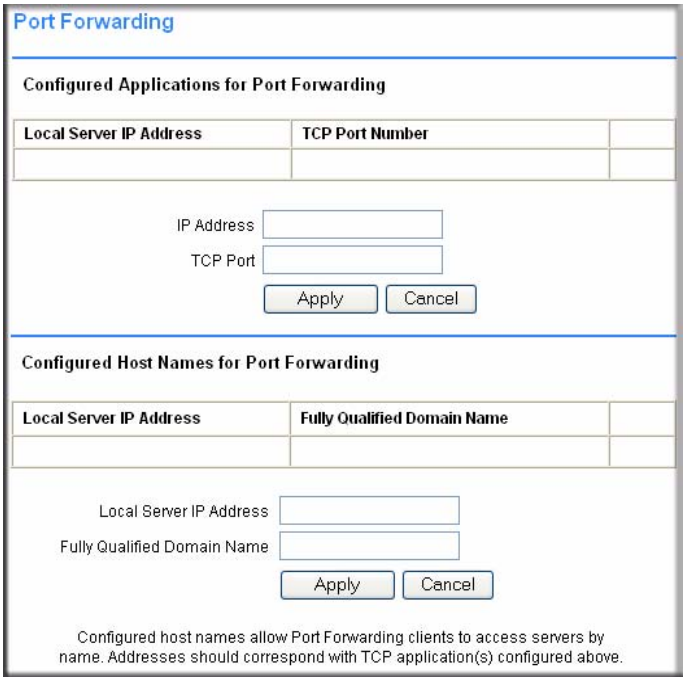

Figure 10-1

2. In the **Configured Applications for Port Forwarding** section, enter the IP address of an internal server or host computer in the **IP Address** field.
3. Enter the TCP port number of the application to be tunneled in the **TCP Port** field. Table 10-1 below lists the more commonly used TCP applications and port numbers (see *http://www.iana.org* for a more complete list of registered port numbers).
4. Click **Apply**. The IP address and port number submitted will appear in the **Configured Applications for Port Forwarding** table.

Table 10-1. Port Forwarding Applications/TCP Port Numbers

TCP Application	Port Number
FTP Data (usually not needed)	20
FTP Control Protocol	21
SSH	22[a]
Telnet	23[b]
SMTP (send mail)	25

Table 10-1. Port Forwarding Applications/TCP Port Numbers (continued)

TCP Application	Port Number
HTTP (web)	80
POP3 (receive mail)	110
NTP (network time protocol)	123
Citrix	1494
Terminal Services	3389
VNC (virtual network computing)	5900 or 5800

a. Users can specify the port number together with the host name or IP address.

b. Ibid.

Configuring Host Name Resolution

Once all the server and port information has been configured, remote users will be able to access private network servers using Port Forwarding. Since users will need to remember the complicated IP addresses of your network servers, the SSL VPN Concentrator administrator can also specify host name to IP address resolution. Once configured, users will be able to access TCP applications at familiar addresses such as “mail.mycompany.com” or “ftp.mycompany.com”.

To add a host name for client name resolution:

1. Enter an IP address in the **Local Server IP Address** field in the **Configured Host Names for Port Forwarding** section. The address should already be defined in the **Configured Applications for Port Forwarding** table.
2. Enter a domain name of the internal server in the **Fully Qualified Domain Name** field.
3. Click **Apply** to submit the host-to-name mapping. The IP address and domain name should appear in the **Configured Host Names for Port Forwarding** table.

   Now, remote users will be able to securely access network applications once they have logged into the SSL VPN portal and launched Port Forwarding.

Appendix A
Default Settings and Technical Specifications

This appendix provides the factory default settings and technical specifications for the ProSafe SSL VPN Concentrator 25.

Factory Default Settings

You can use the reset button located on the front of your device to reset all settings to their factory defaults. This is called a hard reset.

- To perform a hard reset, push and hold the reset button for approximately 5 seconds (until the TEST LED blinks rapidly). Your device will return to the factory configuration settings shown in Table A-1 below.
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

Table A-1. SSL312 Default Configuration Settings

Feature		Description
AP Login		
	User Login URL	192.168.1.1
	User Name (case sensitive)	admin
	Login Password (case sensitive)	password
Ethernet Port 1		
	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Port Speed	10/100
	Gateway Address	0.0.0.0
Ethernet Port 2		
	IP Address	10.0.0.1
	Subnet Mask	255.0.0.0
	Port Speed	10/100

Table A-1. SSL312 Default Configuration Settings

Feature		Description
	Gateway Address	0.0.0.0
Concentrator		
	Ethernet MAC Address	See bottom label.
	Time Zone	GMT
	Time Zone Adjusted for Daylight Saving Time	Automatically enabled if DST available in area selected; otherwise disabled.
	SNMP	SNMPv1 and 2 (MIB2)

Technical Specifications

Table A-2. SSL312 Technical Specifications

Parameter	ProSafe SSL VPN Concentrator 25
Network Management	Web-based configuration and status monitoring
Concurrent Users Supported	25 tunnels
Encryption	DES, 3DES, AES, MD5, SHA-1
Modes	Single ARM and Bridged/routed
Authentication	Local User database, RADIUS, LDAP, MS Active Directory
Certificates supported	X.509, CRL
Aggregate Throughput	6.5 Mbps
Status LEDs	Power/Ethernet LAN1 and LAN2//Test
Electromagnetic Compliance	FCC Part 15 Class B and Class E, CE, and C-TICK
Environmental Specifications	Operating temperature: 0 to 50° C Operating humidity: 5-95%, non-condensing

Appendix B
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Communications	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing a Computer for Network Access	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking (VPN)	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Index

Numerics

A

B

C

H

I

J

L

M

N

P

R

S

T

U

V

W